



JAPANESE PATENT OFFICE

## PATENT ABSTRACTS OF JAPAN

(11)Publication number: 10198739

(43)Date of publication of application: 31.07.1998

(51)Int.Cl.

G06F 17/60  
G07F 7/08  
G09C 1/00  
G09C 1/00  
H04Q 7/38  
// G06F 19/00

(21)Application number: 09117681

(71)Applicant:

MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing: 22.04.1997

(72)Inventor:

TAKAYAMA HISASHI

(30)Priority

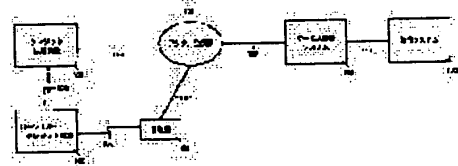
Priority number: 08316897 Priority date: 14.11.1996 Priority country: JP

(54) PERSONAL ELECTRONIC ACCOUNT SETTLEMENT SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an account settling means improve in safety and convenience.

SOLUTION: This system is provided with a paying means 100 equipped with plural systems of communication means, a demanding means 101 equipped with plural systems of communication means, and an account settling means 102 equipped with plural systems of communication means, and among the respective paying means, demanding means and account settling means, communications are performed while using respectively different systems of communication means. By exchanging account settlement information through communications between the paying means and the account settling means, illegal demand due to the demanding means is prevented and by exchanging signatures (digital signatures) or calculation statements through communication between the paying means and the demanding means, sale can be made efficient.



**This Page Blank (uspto)**

Japanese Publication for Unexamined Patent Application  
No. 198739/1998 (Tokukaihei 10-198739)

A. Relevance of the Above-identified Document

This document has relevance to claims 1 and 16 of the present application.

B. Translation of the Relevant Passages of the Document

[ABSTRACT]

[MEANS TO SOLVE THE PROBLEMS]

A personal electric account settlement system, comprising:

paying means 100 having plural systems of communication means;...

[CLAIMS]

[CLAIM 1]

A personal electric account settlement system, comprising:

paying means having plural systems of communication means;

demanding means having plural systems of communication means; and

account settling means having plural systems of communication means,...

[CLAIM 2]

The personal electric account settlement system as

This Page Blank (uspto)



set forth in claim 1, wherein said paying means includes wireless communication means of different kinds...

[CLAIM 3]

The personal electric account settlement system as set forth in claim 2, wherein wireless communication means of said paying means with the demanding means has shorter communication distance and higher directivity than wireless communication means of said paying means with the account settling means.

[CLAIM 4]

The personal electric account settlement system as set forth in claim 2 or 3, wherein wireless communication means of said paying means with the demanding means is optical communication means, and...

[DETAILED DESCRIPTIONS OF THE INVENTION]

[PROBLEMS TO BE SOLVED BY THE INVENTION]

However, in the conventional account settlement system, the sales clerk of retailers had an access to the credit card, and there were cases where the sales clerk, having an access to the credit card number, makes criminal use of the credit card number.

[0013]

Further, in the conventional account settlement system, settlement of accounts proceeded with the

**This Page Blank (uspto)**

initiative of retailers, and there were cases where the retailers cheat on the consumer and initiate the account settlement at the higher price than the actual price.

[0014]

Also, in the conventional account settlement system, the credit card is directly set in the credit settling terminal provided in the retailers, and there were cases where the retailers modify the credit setting terminal to change the information contained in the credit card or illegally read personal information other than ID information of the credit card.

[0015]

Further, the conventional account settlement system required a consumer to carry a credit card for each credit service, which necessitated the inconvenience for the user to carry several credit cards to have a plurality of credit services by contracting with a plurality of credit card companies.

[0016]

Further, the conventional account settlement system employs a credit card as a physical entity for authentication, and thus, in order for the user to cancel the transaction of credit settlement, the user had to experience the inconvenience of returning to the

This Page Blank (uspto)

place where the transaction was made.

[0017]

Further, the conventional account settlement system required to print out the balance sheet, which set the obstacle for efficient sales. Also, it required the credit settling terminal to be equipped with a printer, which made it difficult to reduce the size and cost of the credit settling terminal.

[0018]

Further, the conventional account settlement system required the consumer to sign the balance sheet, and the time it takes for the retailer to ask the consumer for the signature occupied most of the time required for the credit settlement, which set the obstacle for efficient sales.

[0019]

The present invention was made to solve the problems associated with the conventional account settlement system, and its object is to provide account settling means which is safe and easy to use.

[0020]

[MEANS TO SOLVE THE PROBLEMS]

The present invention provides a personal account settlement system which includes paying means having plural systems of communication means, demanding means

This Page Blank (uspto)

having plural systems of communication means, and account setting means having plural systems of communication means (or service offering means having plural systems of communication means and transaction means having a communication network with the service offering means). The paying means, demanding means, and account settling means (or service offering means and transaction means) communicate one another via different systems of communication means.

[0021]

By exchanging account settlement information between the paying means and settling means (or service offering means), unauthorized claim by the demanding means can be prevented. Further, an operator of the demanding means will not have an access to identification information of the paying means or personal information of the owner of the paying means. Also, by exchanging necessary information between the paying means and the demanding means via communication means, efficient sales can be facilitated.

[0022]

[EMBODIMENTS]

The invention of claim 1 of the present invention includes paying means having plural systems of communication means, and...

This Page Blank (uspto)



[0025]

According to the invention of claim 4 of the present invention, the paying means includes optical communication means as the wireless communication means with the demanding means, and includes radio wireless communication means as the wireless communication means with the setting means, wherein the optical wireless communication means such as an infra red ray is used for the near-distance communication between the paying means and the demanding means, while the radio wireless communication means is used for the long-distance communication between the paying means and the settling means.

[0026]

According to the invention of claim 5 of the present invention, the paying means includes..., and input means for allowing entry of payment value,...

[0027]

According to the invention of claim 6 of the present invention, the demanding means includes,..., and input means for allowing entry of demanded value, ...

[0029]

According to the invention of claim 8 of the present invention,... the owner of the paying means

This Page Blank (uspto)

requests account settlement directly to the settling means by specifying the payment value to prevent unauthorized claim by the demanding means, and the owner of the paying means can manage the history of payment (transaction data).

[0031]

According to the invention of claim 10 of the present invention, the central processing unit of the demanding means generates message data for demanding payment of amount corresponding to the value entered by the input means of the demanding means and sends it to the paying means, and generates message data for requesting account settlement from the message data received from the paying means and the message data claiming payment and sends it to the settling means,..., and it is possible to prevent unauthorized claim by the demanding means.

[0032]

According to the invention of claim 11 of the present invention, the central processing unit of the demanding means generates message data for claiming payment and sends it to the paying means, and the central processing unit of the paying means generates message data for requesting a payment process from the message data offering payment and the message data for

**This Page Blank (uspto:**

claiming payment received from the demanding means, and sends it to the settling means, and the settling means conducts a transaction by matching the message data for requesting a transaction received from the demanding means and the message data for requesting a payment process received from the paying means so as to generate message data indicative of completion of account settlement and sends it to the demanding means, and to generate message data indicative of completion of payment and sends it to the paying means.

[0033]

According to the invention of claim 12 of the present invention,..., and it is possible to conduct account settlement without allowing the demanding means to have access to identification information of the paying means, or identification information of the owner of the paying means, thus preventing leaking identification information which corresponds to the credit card number.

[0034]

According to the invention of claim 13 of the present invention, the second storing means of the paying means stores identification information of a plurality of paying means..., and it is not required to carry a plurality of credit cards...

**This Page Blank (uspto)**

[0035]

According to the invention of claim 14 of the present invention, the settling means generates identification information of the owner of the paying means effective for the owner of the demanding means...

[0036]

According to the invention of claim 15 of the present invention, the paying means includes battery capacity detecting means..., and data stored in the paying means will not be erased even when the battery runs out.

[0037]

According to the invention of claim 16 of the present invention, ..., and a large volume of transaction data can be managed even when the capacity of the second storing means of the paying means is small, thus reducing the size of the paying means.

[0038]

According to the invention of claim 17 of the present invention, ..., and the size of the demanding means can be reduced.

[0039]

According to the invention of claim 18 of the present invention, the central processing unit of the paying means generates message data including data

**This Page Blank (usp1c,**



stored in the second storing means of the paying means at the time as specified by the settling means,... to update the data stored in the second storing means of the paying means.

[0040]

According to the invention of claim 19 of the present invention,... It is possible to maintain consistency between data stored in the demanding means and data stored in the settling means.

[0044]

According to the invention of claim 23 of the present invention,..., and when unauthorized change is found, the paying means is inactivated..., thus preventing unauthorized change to the information stored in the paying means.

[0045]

According to the invention of claim 24 of the present invention,..., and unauthorized change to the information stored in the demanding means can be prevented.

[0046]

According to the invention of claim 25 of the present invention, a cancelling operation of the transaction can be made even when the paying means is distanced away from the demanding means.

**This Page Blank (uspto)**

[0048]

According to the invention of claim 27 of the present invention,..., and the privacy of the owner of the paying means can be protected further securely.

[0050]

According to the invention of claim 29 of the present invention,..., and a digital signature of the owner of the paying means is incorporated...

[0051]

According to the invention of claim 30 of the present invention,..., and a digital signature of the owner of the demanding means is incorporated...

[0052]

According to the invention of claim 31 of the present invention, unauthorized account settlement by a faked owner of the settling means can be prevented.

[0053]

According to the invention of claim 32 of the present invention, the paying means includes audio data processing means for converting data received by the communication means into audio data...

[0054]

According to the invention of claim 33 of the present invention,..., and the owner of the demanding means is allowed to talk to the customer...

**This Page Blank (uspto)**

[0055]

According to the invention of claim 34 of the present invention,..., and it is possible to protect privacy, for example, from tapping.

[0058]

According to the invention of claim 37 of the present invention,..., and the demanding means effects an enveloping process to prevent unauthorized claim by a faked owner of the demanding means...

[0060]

According to the invention of claim 39 of the present invention,..., and lost data can be restored.

[0061]

According to the invention of claim 40 of the present invention,..., and the system can be constructed without major modification to the conventional transaction means...

[0063]

According to the invention of claim 42 of the present invention,..., and the system can be constructed without major modification to the conventional transaction means...

[0066]

According to the invention of claim 45 of the present invention,..., the transaction means is

**This Page Blank (uspto)**

selected from a plurality of transaction means...

[0069]

According to the invention of claim 49 of the present invention,..., and information relating to privacy of the user in the account settlement can be managed safely and efficiently.

[0070]

According to the invention of claim 50 of the present invention,..., and effective period information is incorporated,..., and each effective period information is verified, thus preventing an unauthorized request using old message data.

[0072]

According to the invention of claim 52 of the present invention,..., and photograph information and age information of the owner of the paying means are included, and... the owner of the paying means can be confirmed.

[0073]

According to the invention of claim 53 of the present invention, when the free space AU of the second storing means of the paying means becomes less than (AU > 0), ...

[0074]

According to the invention of claim 54 of the

**This Page Blank (uspto)**



present invention, when the free space AM of the second storing means of the demanding means becomes less than  $(AM > 0)$ , ...

[0075]

According to the invention of claim 55 of the present invention,..., and the control program of the paying means can always be updated to the newest version...

[0076]

According to the invention of claim 56 of the present invention,..., and the control program of the demanding means can always be updated to the newest version...

[0077]

According to the invention of claim 57 of the present invention, the settling means or service offering means incorporates identification information of the transaction... in the message data indicative of completion of payment,..., and a request for unauthorized cancellation can be prevented.

[0078]

According to the invention of claim 58 of the present invention,..., a request for unauthorized cancellation can be prevented,..., and lost data can be restored even when the paying means or demanding means

**This Page Blank (uspto)**

fails...

[0079]

According to the invention of claim 60 of the present invention,..., the owner of the paying means and the owner of the demanding means can talk to each other...

[0080]

According to the invention of claim 61 of the present invention, the paying means and the demanding means exchange secret keys...

[0081]

According to the invention of claim 62 of the present invention, the calculator system of the service offering means includes user information processing means...; merchant information processing means...; transaction processor information processing means...; and service director information processing means...

[0082]

According to the invention of claim 63 of the present invention, the calculator system of the service offering means includes service manager information processing means for generating or erasing...

[0083]

According to the invention of claim 64 of the present invention, the service manager information

**This Page Blank (vsoto)**

processing means generates user information processing means, corresponding one to one to each paying means...

[0084]

According to the invention of claim 65 of the present invention, the service manager information processing means defines a group of information processing means for carrying out coordination process...

[0085]

According to the invention of claim 66 of the present invention, the service director information... requests addition to a group of the information processing means...

[0086]

According to the invention of claim 67 of the present invention,..., reliability of the system can be improved without processing information having no relevance...

[0087]

According to the invention of claim 68 of the present invention,..., and it is possible to prevent connection between the demanding means and the service offering means by an unauthorized faked owner...

[0088]

According to the invention of claim 69 of the

**This Page Blank (uspto)**

present invention,..., and it is possible to prevent operation by a faked owner...

[0089]

According to the invention of claim 70 of the present invention,..., and it is possible to protect privacy in transactions, for example, from tapping...

[0090]

According to the invention of claim 71 of the present invention,..., and it is possible to prevent unauthorized operation by a faked owner...

[0091]

According to the invention of claim 72 of the present invention, the merchant information processing means having received the message data for requesting a transaction from the demanding means..., and the service director information processing means requests the service manager information processing means to add transaction means to a group of the transaction processor information processing means corresponding to the transaction means selected...

[0092]

According to the invention of claim 73 of the present invention, the merchant information processing means having received the message data for requesting cancellation of a transaction from the demanding

**This Page Blank (uspto)**



means...

[0093]

According to the invention of claim 74 of the present invention, the demanding means uses identification information included in the message data indicative of completion of account settlement...

[0094]

According to the invention of claim 75 of the present invention, the paying means generates message data for requesting communication with the demanding means...

[0095]

According to the invention of claim 76 of the present invention, the settling means or service offering means generates message data for requesting update of data..., and the service offering means can forcibly update information..., which is effective when the content of the contract has been changed...

[0096]

According to the invention of claim 77 of the present invention,..., and the process of the settling means is scattered...

[0097]

According to the invention of claim 78 of the present invention,..., and the process of the settling

**This Page Blank (uspto)**

means is scattered based on area or organization...

[0098]

According to the invention of claim 79 of the present invention,..., the paying means or demanding means can access to information via communication with any settling means...

[0099]

According to the invention of claim 80 of the present invention,..., the process of the service offering means is scattered...

[0100]

According to the invention of claim 81 of the present invention,..., the process of the service offering means is scattered based on area or organization...

[0101]

According to the invention of claim 82 of the present invention,... the information which relates to the paying means and owner of the paying means is stored in the first storing means of the service offering means having the same attribute as the paying means and the owner of the paying means..., and position information indicative of the position where the information which relates to the paying means and owner of the paying means is stored...

**This Page Blank (uspto)**

[0102]

According to the invention of claim 83 of the present invention, the attribute is "organization"...

[0103]

According to the invention of claim 84 of the present invention, the attribute is "area"...

[0104]

According to the invention of claim 85 of the present invention,..., when the home user information processing means is generated on the first service offering means, the mobile user information processing means corresponding to the paying means is generated on the second service offering means so that the mobile user information processing means thus generated and the home user information processing means communicate with the paying means and process information which relates to the paying means and the owner of the paying means in a coordinated manner...

[0105]

According to the invention of claim 86 of the present invention,..., and it is possible to cancel at home, for example, electric account settlement which was made abroad.

[0106]

According to the invention of claim 87 of the

**This Page Blank (uspto)**

present invention,..., the demanding means can also communicate with paying means which is administered by other service offering means.

[0107]

According to the invention of claim 88 of the present invention,..., the paying means can communicate with the demanding means by connecting itself with any service offering means via the communication network as with the case of connecting itself with service offering means storing information which relates to the paying means and information which relates to the owner of the paying means.

[0114]

The following will describe embodiments of the present invention with reference to the drawings.

[0127]

Basically, the service offering system 102 receives a payment request and a settlement request respectively from the personal credit terminal 100 and credit settlement device 101, and matches the payment request and settlement request thus received to request a transaction to the settlement system 103 for the user and merchant.

[0166]

First, the flow of "settlement" process will be

**This Page Blank (uspto)**



described.

[0167]

Fig. 6 shows the flow of "settlement" process in a personal remote credit settlement service. Also, Figs. 7(a) through 7(h) show an exemplified display of the LCD 203 of the personal credit terminal 100 in the "settlement" process, and Figs. 8(a) through 8(g) show an exemplified display of the LCD 302 of the credit settling terminal 300.

[0171]

The user selects a credit card to be used for making payment.

[0525]

The personal remote credit settlement system includes..., and settlement system 103 for conducting a credit transaction in a credit service company or transaction company...

[0530]

The user has a contract with a credit card company for the membership of a credit service, and with a company offering a personal remote credit settlement service for the membership of the personal remote credit settlement service...

[0531]

The company offering a personal remote credit

This Page Blank

settlement service has a contract with a single or plurality of credit card companies to offer a personal remote credit settlement service for the members of the credit service instead of the credit card companies by issuing an electric credit card.

[1487]

The demanding means sends a message of payment request to the paying means, and the paying means sends a message of offering payment to the demanding means, and the demanding means and paying means generate a message of settlement request or payment request, incorporating the information contained in the message thus received, and send it to the settling means (or service offering means), and the settling means (or service offering means) matches these request messages to prevent unauthorized claim by the demanding means and incorrect payment by the paying means. Further, account settlement can be made without allowing the demanding means to have access to the identification number of the paying means or phone number of the owner of the paying means.

**This Page Blank (uspto)**

(11) 日本国特許庁 (J P) (12) 公開特許公報 (A)

(11) 特許公開番号

特開平10-198739

(43) 公開日 平成10年(1998) 7月31日

(51) Int. Cl.		識別記号	
G 0 6 F	17/60	P 1	
G 0 7 F	7/08	G 0 6 F	16/21
G 0 9 C	1/00	G 0 9 C	1/00
			3 4 0 A
			8 4 0 B
			6 6 0 B
			2
H 0 4 Q	7/38	G 0 7 F	7/08
		H 0 4 B	7/29
			1 0 6 H

審査請求 未請求 特許請求の範囲 34 P D (全 207 頁) 最終頁に続く

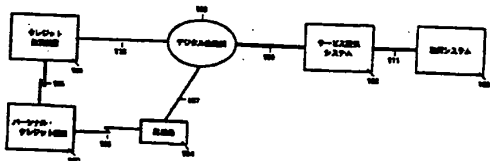
(21) 出願番号	特開平9-117681	(71) 出願人	000065821
(22) 出願日	平成9年(1997) 4月22日	松下電器産業株式会社	
(31) 優先権主張番号	特開平8-316887	大阪府大阪市大字門真1006番地	
(32) 優先日	平8(1996) 11月14日	高山 久	
(33) 優先権主張国	日本 (J P)	大阪府大阪市大字門真1006番地 松下電器産業株式会社内	
(70) 代理人	弁護士 役 高明 (外 3 名)		

(54) 発明の名称 ハーソナル電子決済システム

(57) 要約

(発明) 安全性と利便性に優れた決済手段を提供する。

(解決手段) 複数の系統の通信手段を具備する支払手段100と、複数の系統の通信手段を具備する請求手段101とを、複数の系統の通信手段を具備する決済手段102とを介して、支払手段、請求手段及び決済手段の各々の間における通信を、それぞれ異なる系統の通信手段を用いて行なう。支払手段と決済手段との間の通信で決済情報を交換することにより、請求手段による不正な請求を防ぎ、支払手段と請求手段との間の通信でサイン(デジタル署名)や計算値を交換することにより、販売の効率化を図ることができる。



(特許請求の範囲)

(請求項1) 複数の系統の通信手段を具備する支払手段と、複数の系統の通信手段を具備する請求手段と、複数の系統の通信手段を具備する決済手段とを介して、支払手段、請求手段及び決済手段の各々の間における通信を、それぞれ異なる系統の通信手段を用いて行なうことを特徴とするハーソナル電子決済システム。

(請求項2) 前記支払手段が、前記請求手段及び決済手段と通信するための前記通信手段として、異なる種類の無線通信手段を具備することを特徴とする請求項1に記述のハーソナル電子決済システム。

(請求項3) 前記支払手段が具備する前記請求手段との間の無線通信手段が、前記支払手段との間の無線通信手段に比べて、通信可能な距離が短く、指向性が高い無線通信手段であることを特徴とする請求項2に記述のハーソナル電子決済システム。

(請求項4) 前記支払手段が具備する前記請求手段との間の無線通信手段が無線通信手段であり、前記支払手段が具備する前記決済手段との間の無線通信手段がラジオ無線通信手段であることを特徴とする請求項2または3に記述のハーソナル電子決済システム。

(請求項5) 前記支払手段が、前記無線通信手段及びラジオ無線通信手段と、支払金額の値を入力する入力手段と、前記無線通信手段及びラジオ無線通信手段によって送信されるデータの生成処理と前記無線通信手段及びラジオ無線通信手段によって受信されたデータの処理とを行なう中央処理装置と、前記中央処理装置の動作を制御する制御プログラムを記憶する第1の記憶手段と、前記中央処理装置によるデータの処理の結果を表示する表示手段と、前記中央処理装置によって処理されたデータを蓄積する第2の記憶手段とを具備することを特徴とする請求項4に記述のハーソナル電子決済システム。

(請求項6) 前記請求手段が、前記支払手段との間で通信を行なう光通信手段と、前記決済手段との間で通信を行なう通信手段と、請求する金額の値を入力する入力手段と、前記無線通信手段及びラジオ無線通信手段によって送信されるデータの生成処理と前記無線通信手段及びラジオ無線通信手段によって受信されたデータの処理とを行なう中央処理装置と、前記中央処理装置の動作を制御する制御プログラムを記憶する第1の記憶手段と、前記中央処理装置によるデータの処理の結果を表示する表示手段と、前記中央処理装置によって処理されたデータを蓄積する第2の記憶手段とを具備することを特徴とする請求項1乃至5に記述のハーソナル電子決済システム。

(請求項7) 前記決済手段が、前記支払手段に関する情報を蓄積する第1の記憶手段と、前記請求手段に関する情報を蓄積する第2の記憶手段と、決済処理におけるデータ処理を行なう計算機システムとを具備することを特徴とする請求項1乃至6に記述のハーソナル電子決済システム。

(2)

(請求項8) 前記支払手段の中央処理装置が、前記支払手段の入力手段によって入力された値に相当する金額の支払処理を要求するメッセージデータを生成して前記決済手段に送信し、また、前記決済手段から受信した支払の完了を示すメッセージデータを処理して、前記支払の完了を出力し、さらに、前記処理したデータを支払手段の前記第2の記憶手段に格納することを特徴とする請求項1乃至7に記述のハーソナル電子決済システム。

(請求項9) 前記支払手段の中央処理装置が、前記支払手段の入力手段によって入力された値に相当する金額の支払を申し出るメッセージデータを生成して前記請求手段に送信することを特徴とする請求項1乃至8に記述のハーソナル電子決済システム。

(請求項10) 前記請求手段の中央処理装置が、前記請求手段の入力手段によって入力された値に相当する金額の支払を請求するメッセージデータを生成して前記支払手段に送信し、前記支払手段から受信した支払を申し出るメッセージデータと、前記支払手段を請求するメッセージデータとから、決済処理を要求するメッセージデータを生成して前記決済手段に送信し、また、前記決済手段から受信した決済の完了を示すメッセージデータを処理して、請求手段の前記表示手段に出力し、さらに、前記処理したデータを請求手段の前記第2の記憶手段に格納することを特徴とする請求項1乃至9に記述のハーソナル電子決済システム。

(請求項11) 前記請求手段の中央処理装置が、支払を請求するメッセージデータを生成して前記支払手段に送信し、前記支払手段の中央処理装置が、生成した支払を申し出るメッセージデータと、前記請求手段から受信した支払を請求するメッセージデータとから支払処理を要求するメッセージデータを生成して前記決済手段に送信し、前記決済手段が、前記請求手段から受信した決済の完了を示すメッセージデータを処理して、請求手段の前記表示手段に出力し、さらに、前記処理したデータを請求手段の前記第2の記憶手段に格納することを特徴とする請求項1乃至10に記述のハーソナル電子決済システム。

(請求項12) 前記支払手段の中央処理装置が、前記支払を申し出るメッセージデータの中にそのメッセージデータを識別する識別情報を入れ、前記支払処理を要求するメッセージデータの中に、前記支払を申し出るメッセージデータの識別情報と、支払手段の識別情報とを入れ、前記請求手段の中央処理装置が、前記支払を請求するメッセージデータの中にそのメッセージデータを識別する識別情報を入れ、前記決済処理を要求するメッセージデータの中に、前記支払を請求するメッセージデータの識別情報と、請求手段の識別情報と、前記支払を申し

(3)

出るメッセージデータの識別情報とを入れ、前記決済手段が、前記支払処理を要求するメッセージデータ及び決済処理を要求するメッセージデータの中の前記支払を申し出るメッセージデータの識別情報と前記支払を請求するメッセージデータの識別情報とを照合することを特徴とする請求項8乃至11に記載のパーソナル電子決済システム。

【請求項13】 前記支払手段の第2の蓄積手段には、複数の支払方法の識別情報が格納され、前記支払手段の中央処理装置が、前記支払手段の入力手段によって選択された前記支払方法の識別情報を、前記支払を申し出るメッセージデータ及び支払を請求するメッセージデータの中に入れて、前記決済手段の第2の蓄積手段に蓄積することを特徴とする請求項8乃至12に記載のパーソナル電子決済システム。

【請求項14】 前記決済手段が、前記請求手段の所有者に対して有効な前記支払手段の所有者の識別情報を生成し、決済の完了を要するメッセージデータの中に入れて、前記請求手段に送信することを特徴とする請求項1乃至13に記載のパーソナル電子決済システム。

【請求項15】 前記支払手段が、前記支払手段のバックテリ容量を抽出するバッテリ特異抽出手段を具備し、前記バックテリ容量がQ (Q>0) 以下になったとき、前記支払手段の中央処理装置が、前記中央処理装置によって処理されたデータが蓄積された支払手段の前記第2の蓄積手段のデータと前記決済手段に送信し、前記決済手段が、受信した前記データを、前記支払手段に関する情報を蓄積する決済手段の第1の蓄積手段に蓄積することを特徴とする請求項1乃至14に記載のパーソナル電子決済システム。

【請求項16】 前記支払手段の中央処理装置によって処理されたデータが、前記支払手段の第2の蓄積手段、または前記決済手段の支払手段に関する情報を蓄積する第1の蓄積手段に蓄積され、これらのデータが、前記支払手段の第2の蓄積手段に、前記データの識別情報と、前記データの存在する蓄積手段上のアドレスとを記述し管理され、前記決済手段の第1の蓄積手段上のアドレスを示すデータを処理する場合に、前記支払手段の中央処理装置が、前記データを要求するメッセージデータを生成して前記決済手段に送信し、前記メッセージデータを受信した決済手段が、要求されたデータを含むメッセージデータを生成して支払手段に送信し、支払手段の中央処理装置が、前記決済手段から受信したメッセージデータを要求したデータを取り出すことを特徴とする請求項1乃至15に記載のパーソナル電子決済システム。

【請求項17】 前記請求手段の中央処理装置によって処理されたデータが、前記請求手段の第2の蓄積手段、または前記決済手段の請求手段に関する情報を蓄積する第2の蓄積手段に蓄積され、これらのデータが、前記請求手段の第2の蓄積手段に、前記データの識別情報と、前記データの存在する蓄積手段上のアドレスとを記述し

を特徴とする請求項18に記載のパーソナル電子決済システム。

【請求項22】 前記決済手段が、前記請求手段から請求手段の前記第2の蓄積手段に蓄積されているデータを包含メッセージデータを受信して、請求手段の前記第2の蓄積手段の更新データを生成する際に、データの生成時刻と比較し、生成時刻が遅いデータに対して、前記請求手段の第2の蓄積手段上のアドレスを割り当て、生成時刻が早いデータに対して、前記請求手段の請求手段に関する情報を蓄積する第2の蓄積手段上のアドレスを割り当てて、前記請求手段の第2の蓄積手段に蓄積することを特徴とする請求項19に記載のパーソナル電子決済システム。

【請求項23】 前記決済手段が、前記支払手段から支払手段の前記第2の蓄積手段に蓄積されているデータを含むメッセージデータを受信したとき、前記メッセージデータから取り出した支払手段の前記第2の蓄積手段に関する情報を蓄積する第1の蓄積手段に蓄積されているデータとを照合して、不正な改ざんが検出された場合に、前記支払手段の検出を中止させるメッセージデータを前記支払手段に送信することを特徴とする請求項16、18、20または21に記載のパーソナル電子決済システム。

【請求項24】 前記決済手段が、前記請求手段から前記第2の蓄積手段に蓄積されているデータを含むメッセージデータを受信したとき、前記メッセージデータから取り出した前記第2の蓄積手段に蓄積されているデータと、前記決済手段の請求手段に関する情報を蓄積する第2の蓄積手段に蓄積されているデータとを照合して、不正な改ざんが検出された場合に、前記請求手段の機能を停止させるメッセージデータを前記請求手段に送信することを特徴とする請求項17、19または22に記載のパーソナル電子決済システム。

【請求項25】 前記支払手段の中央処理装置が、支払手段の完了を要するメッセージデータを用いて、支払処理の取消処理を要求するメッセージデータを生成して前記決済手段に送信し、前記請求手段の中央処理装置が、決済の完了を示すメッセージデータを用いて、決済処理の取消処理を要求するメッセージデータを生成して前記決済手段に送信し、前記決済手段が、前記支払手段及び請求手段のそれぞれから受信した前記メッセージデータを照合して、決済処理の取消処理を行ない、前記支払手段に支払処理の取消処理の完了を要するメッセージデータを送信し、前記請求手段に決済処理の取消処理の完了を要するメッセージデータを送信することを特徴とする請求項1乃至24に記載のパーソナル電子決済システム。

【請求項26】 前記請求手段の中央処理装置が、前記決済手段から受信した決済の完了を要するメッセージデータの中が含まれる支払手段の所有者の識別情報をを用いて、前記支払手段との通信を要求するメッセージデータ

(4)

を生成して前記決済手段に送信し、前記決済手段が、前記支払手段に対して、前記請求手段との通信回線の接続を知らせるメッセージデータを生成して送信し、さらに、前記識別情報から識別した前記支払手段と前記請求手段との通信回線を接続し、前記支払手段の中央処理装置が、前記メッセージデータを受信して、支払手段の表示手段に、前記請求手段の所有者の識別情報と、前記請求手段との通信回線の接続状態とを表示することを特徴とする請求項14乃至25に記載のパーソナル電子決済システム。

【請求項27】 前記決済手段が、前記支払手段と前記請求手段との通信回線を接続するとき、前記決済手段の第1の蓄積手段に蓄積されている前記支払手段の所有者が設定したアクセス制御情報を参照して、前記請求手段からのアクセスが禁止されている場合には、前記通信回線を接続しないことを特徴とする請求項26に記載のパーソナル電子決済システム。

【請求項28】 前記支払手段の中央処理装置が、前記決済手段から受信した決済の完了を要するメッセージデータを用いて、前記請求手段との通信を要求するメッセージデータを生成して前記決済手段に送信し、前記決済手段が、前記請求手段に対して、決済の完了を要するメッセージデータに含まれる前記支払手段の所有者の識別情報を含み、前記支払手段との通信回線の接続を知らせるメッセージデータを生成して送信し、さらに、前記支払手段と前記請求手段との通信回線を接続し、前記請求手段の中央処理装置が、前記メッセージデータを受信して、請求手段の表示手段に、前記支払手段の所有者の識別情報と、前記支払手段との通信回線の接続状態とを表示することを特徴とする請求項14乃至27に記載のパーソナル電子決済システム。

【請求項29】 前記支払手段が、前記請求手段または前記決済手段へ送信する前記メッセージデータに、支払手段の所有者のデジタル署名を施すことを特徴とする請求項1乃至28に記載のパーソナル電子決済システム。

【請求項30】 前記請求手段が、前記支払手段または前記決済手段へ送信する前記メッセージデータに、請求手段の所有者のデジタル署名を施すことを特徴とする請求項1乃至29に記載のパーソナル電子決済システム。

【請求項31】 前記決済手段が、前記支払手段または前記請求手段へ送信する前記メッセージデータに、決済手段の所有者のデジタル署名を施すことを特徴とする請求項1乃至30に記載のパーソナル電子決済システム。

【請求項32】 前記支払手段が、音声入力手段と、音声出力手段と、前記音声入力手段から入力される音声データを前記通信手段で送信するデータを変換し、且つ、前記通信手段で受信されたデータを前記変換出力手段によって出力される音声データへ変換する音声データ処理手段とを具備することを特徴とする請求項1乃至31に記載のパーソナル電子決済システム。

(5)

- 【請求項33】 前記請求手段が、音声入力手段と、音声出力手段と、前記音声入力手段から入力される音声データを前記通信手段で送信されるデータへ変換し、且つ、前記通信手段で受信されたデータを前記音声出力手段によって出力される音声データへ変換する音声データ処理手段とを具備することを特徴とする請求項1乃至32に記載のパターン電子決済システム。
- 【請求項34】 前記支払手段が、送信するメッセージデータの暗号化処理と受信したメッセージデータの暗号の復号化処理とを行なう暗号処理手段と、送信する音声データの暗号化処理と受信した音声データの暗号の復号化処理とを行なう音声暗号処理手段とを具備することを特徴とする請求項1乃至33に記載のパターン電子決済システム。
- 【請求項35】 前記請求手段が、送信するメッセージデータの暗号化処理と受信したメッセージデータの暗号の復号化処理とを行なう暗号処理手段と、送信する音声データの暗号化処理と受信した音声データの暗号の復号化処理とを行なう音声暗号処理手段とを具備することを特徴とする請求項1乃至34に記載のパターン電子決済システム。
- 【請求項36】 前記支払手段が、前記決済手段へ送信する前記メッセージデータに、支払手段の所有者のデジタル署名を施すとともに、前記決済手段の所有者に対して暗号化処理を施すことを特徴とする請求項1乃至35に記載のパターン電子決済システム。
- 【請求項37】 前記請求手段が、前記決済手段へ送信する前記メッセージデータに、請求手段の所有者のデジタル署名を施すとともに、前記決済手段の所有者に対して暗号化処理を施すことを特徴とする請求項1乃至36に記載のパターン電子決済システム。
- 【請求項38】 前記決済手段が、前記支払手段へ送信する前記メッセージデータに、決済手段の所有者のデジタル署名を施すとともに、前記支払手段の所有者に対して暗号化処理を施し、また、前記請求手段へ送信する前記メッセージデータに、決済手段の所有者のデジタル署名を施すとともに、前記請求手段の所有者に対して暗号化処理を施すことを特徴とする請求項1乃至37に記載のパターン電子決済システム。
- 【請求項39】 前記決済手段が、前記請求手段に送信した決済の完了を返すメッセージデータを、請求手段に送る情報とを施す決済手段の前記第2の着払手段に送信し、支払手段に送信した支払の完了を返すメッセージデータを、支払手段に関する情報を施す決済手段の前記第1の着払手段に送信することを特徴とする請求項1乃至38に記載のパターン電子決済システム。
- 【請求項40】 前記決済手段が、前記支払手段との通信手段及び前記請求手段との通信手段を介して前記支払手段の所有者及び前記請求手段の所有者に電子決済サービスを提供するサービス提供手段と、前記サービス提供手段と通信手段を介して隣接し、前記支払手段の所有者及び前記請求手段の所有者の間の決済処理を実行する決済処理手段とから成ることを特徴とする請求項1乃至39に記載のパターン電子決済システム。
- 【請求項41】 前記サービス提供手段が、前記支払手段及び支払手段の所有者に関する情報を施す第1の着払手段と、前記請求手段及び請求手段の所有者に関する情報を施す第2の着払手段と、電子決済サービスを提供するためのデータ処理を行なう計算機システムとを具備することを特徴とする請求項40に記載のパターン電子決済システム。
- 【請求項42】 前記決済処理手段が、前記支払手段の所有者の決済処理に関する情報を施す第1の着払手段と、前記請求手段の所有者の決済処理に関する情報を施す第2の着払手段と、決済処理におけるデータ処理を行なう計算機システムとを具備することを特徴とする請求項40または41に記載のパターン電子決済システム。
- 【請求項43】 前記サービス提供手段が、前記請求手段から送信された決済処理を要求する前記メッセージデータと前記支払手段から送信された支払処理を要求する前記メッセージデータを照合し、決済実行処理を要求するメッセージデータを生成して前記決済処理手段に送信し、決済処理を実行した前記決済処理手段が、決済処理の完了を返すメッセージデータを生成して前記サービス提供手段に送信し、前記サービス提供手段が、決済処理の完了を返す前記メッセージデータから決済の完了を返すメッセージデータと支払の完了を返すメッセージデータを生成して、それぞれを前記請求手段と前記支払手段とへ送信することを特徴とする請求項40乃至42に記載のパターン電子決済システム。
- 【請求項44】 前記サービス提供手段が、前記請求手段に送信した決済の完了を返すメッセージデータをサービス提供手段の前記第2の着払手段に送信し、支払手段に送信した支払の完了を返すメッセージデータをサービス提供手段の前記第1の着払手段に送信することを特徴とする請求項41乃至43に記載のパターン電子決済システム。
- 【請求項45】 前記決済処理手段が、取り扱う決済処理の情報を照合する複数の決済処理手段によって構成され、前記サービス提供手段が、前記決済処理手段に関する情報を施す第3の着払手段を具備していることを特徴とする請求項41乃至44に記載のパターン電子決済システム。
- 【請求項46】 前記サービス提供手段が、前記決済処理を要求するメッセージデータと前記支払処理を要求するメッセージデータとの照合結果に基づいて、前記決済実行処理を要求するメッセージデータを送る決済処理手段と、複数の決済処理手段の中から選択することを特徴とする請求項45に記載のパターン電子決済システム。

(6)

- 4.
- 【請求項47】 前記サービス提供手段が、前記決済処理手段から受信した決済処理の完了を返すメッセージデータを、サービス提供手段の前記第3の着払手段に送信することを特徴とする請求項45または46に記載のパターン電子決済システム。
- 【請求項48】 前記サービス提供手段の前記第1の着払手段に送信される支払手段の所有者に関する情報の中に、支払手段の所有者の決済処理に関する情報と、支払手段の所有者に帰属する情報とが含まれ、前記サービス提供手段の前記第2の着払手段に送信される請求手段の所有者に関する情報の中に、請求手段の所有者の決済処理に関する情報と、請求手段の所有者に帰属する情報とが含まれることを特徴とする請求項47に記載のパターン電子決済システム。
- 【請求項49】 前記サービス提供手段の第1の着払手段の情報は、前記支払手段の所有者ごとに管理して蓄積され、前記サービス提供手段の第2の着払手段の情報は、前記請求手段の所有者ごとに管理して蓄積されることを特徴とする請求項41乃至48に記載のパターン電子決済システム。
- 【請求項50】 前記支払手段の中央処理装置が、前記支払を申し出るメッセージデータ及び前記支払処理を要求するメッセージデータの中に、そのメッセージデータの有効期間情報を入れ、前記請求手段の中央処理装置が、前記支払を請求するメッセージデータ及び前記決済処理を要求するメッセージデータの中に、そのメッセージデータの有効期間情報を入れ、前記請求手段または前記サービス提供手段が、前記支払処理を要求するメッセージデータと決済処理を要求するメッセージデータとを照合する際に、前記各有効期間情報を検証することを特徴とする請求項1乃至49に記載のパターン電子決済システム。
- 【請求項51】 前記請求手段の中央処理装置が、前記決済処理を要求するメッセージデータを生成する前に、前記支払手段の所有者の照会処理を要求するメッセージデータを生成して前記サービス提供手段へ送信し、前記サービス提供手段が、前記支払処理を要求するメッセージデータと前記照会処理を要求するメッセージデータとを照合して、サービス提供手段の前記第1の着払手段に送信された支払手段の所有者に関する情報と、前記所有者の照会結果を示すメッセージデータを生成して前記請求手段へ送信し、前記請求手段の中央処理装置が、このメッセージデータを処理して、請求手段の表示手段に出力することを特徴とする請求項41乃至50に記載のパターン電子決済システム。
- 【請求項52】 前記サービス提供手段の前記第1の着払手段に送信される支払手段の所有者に関する情報の中に、支払手段の所有者の写真情報と年齢情報とが含まれ、前記サービス提供手段が、前記所有者の照会結果を示すメッセージデータの中に、前記請求手段の中央処理装置が、前記請求手段の所有者の写真情報と年齢情報とを照合するときに、前記サービス提供手段の所有者の間の決済処理を実行する決済処理手段とから成ることを特徴とする請求項51に記載のパターン電子決済システム。
- 【請求項53】 前記支払手段の前記第2の着払手段の空き容量が、 $AV(AV>0)$ 未満になった場合に、支払手段の中央処理装置が、支払手段の前記第2の着払手段に蓄積されているデータを含むメッセージデータを生成して前記決済手段または前記サービス提供手段に送信し、前記サービス提供手段が、支払手段の前記第2の着払手段の更新データを含むメッセージデータを生成して前記支払手段に送信し、前記支払手段の中央処理装置が、前記決済手段または前記サービス提供手段から受信した前記メッセージデータから更新データをとり出して、支払手段の前記第2の着払手段に蓄積されているデータを更新することを特徴とする請求項1乃至52に記載のパターン電子決済システム。
- 【請求項54】 前記請求手段の前記第2の着払手段の空き容量が、 $AW(AW>0)$ 未満になった場合に、請求手段の中央処理装置が、請求手段の前記第2の着払手段に蓄積されているデータを含むメッセージデータを生成して前記決済手段または前記サービス提供手段に送信し、前記サービス提供手段が、請求手段の前記第2の着払手段の更新データを含むメッセージデータを生成して前記請求手段に送信し、前記請求手段の中央処理装置が、前記決済手段または前記サービス提供手段から受信した前記メッセージデータから更新データをとり出して、請求手段の前記第2の着払手段に蓄積されているデータを更新することを特徴とする請求項1乃至53に記載のパターン電子決済システム。
- 【請求項55】 前記支払手段から支払手段の前記第2の着払手段に蓄積されているデータを含むメッセージデータを受信した、前記決済手段または前記サービス提供手段が、支払手段の前記第2の着払手段と含む新しい支払手段の中央処理装置の制御プログラムとを含むメッセージデータを生成して前記支払手段に送信し、前記サービス提供手段が、支払手段の中央処理装置が、前記決済手段または前記サービス提供手段から受信した前記メッセージデータと前記新しい支払手段の中央処理装置の制御プログラムとを含むメッセージデータを生成して前記請求手段に送信し、前記請求手段の中央処理装置が、前記請求手段の所有者の間の決済処理を実行する決済処理手段とから成ることを特徴とする請求項54に記載のパターン電子決済システム。
- 【請求項56】 前記請求手段から請求手段の前記第2の着払手段に蓄積されているデータを含むメッセージデータを受信した、前記決済手段または前記サービス提供手段が、請求手段の前記第2の着払手段の更新データと新しい請求手段の中央処理装置の制御プログラムとを含むメッセージデータを生成して前記請求手段に送信し、前記請求手段の中央処理装置が、前記請求手段の所有者の間の決済処理を実行する決済処理手段とから成ることを特徴とする請求項55に記載のパターン電子決済システム。

(7)

装置が、新しい請求手段の中央処理装置の制御プログラムと、請求手段の第1の蓄積手段または第2の蓄積手段に蓄積して、その制御プログラムを実行することを特徴とする請求項1乃至5に記載のパーソナル電子決済システム。

【請求項57】 前記決済手段または前記サービス提供手段が、前記決済の完了を教示メッセージデータ中に、決済処理要領及び決済情報を含む前記決済要求手段の識別情報を入れ、前記決済手段及び前記決済情報の取消処理の要領と装置間が、前記支払処理または決済処理の取消処理を要求するそれぞれのメッセージデータの中に、前記決済手段または前記サービス提供手段が、前記支払手段及び前記決済手段のそれぞれから受領した支払処理要領及び決済処理の取消処理を要求する各メッセージデータを照合することと特徴とする請求項2乃至56に記載のパフォーマンス向上型電子決済システム。

【請求項58】 前記サービス提供手段が、前記支払手段の段階及び請求手段のそれぞれから受信した支払処理及び決済処理の取消処理を要求する各メッセージデータを照会して、取消処理の取消処理を要求する前記支払手段のメッセージデータとサービス提供手段の第1の決済手段のメッセージデータとを照会している支払の完了を該サービス手段に通知する段階、及び、決済処理の取消処理を要求する前記サービス手段の第2の決済手段に該サービス手段とサービス提供手段の間の決済手段に通知されている決済の完了を該サービス手段に通知する段階を含むことを特徴とする請求項4乃至57に記載のシステム。

【請求項59】 前記サービス提供手段が、前記請求項57の段階に達していた決済処理の完了を表すメッセージデータをサージャナに送信し、前記請求項2の決済手段に請求データをサージャナに送信し、前記請求項4乃至請求項58に記載の決済手段の取組処理の完了を待機し、支払手段に送信した支払処理の取組処理の完了を待機する請求項4乃至請求項58に記載の決済手段に特徴とするシステム。

【請求項60】 前記決済手段または前記サーバ・システムによる決済手段によって通信回線を接続された前記支払手段と前記決済手段とが、音声データ通信を行なうことを特徴とする決済システム。

【請求項61】 前記決済手段または前記サービス提供手段によって信用回線を接続された前記支払手段と前記手段とが、暗号鍵を交換して、互いに音声データを暗号化して音声データ通信を行なうことを特徴とする請求35乃至60に記載のパーソナル電子決済システム。

【請求項62】 前記サービス提供手段の計算機システムが、前記支払手段との通信とサービス提供手段の第1の業務手段に蓄積される情報の処理とを行なうユーザの報告手段と、前記請求手段との通信とサービス提供手段の第2の業務手段に蓄積される情報の処理とを行な

マーチャント情報処理手段と、前記決済処理手段との通信とサービス提供手段の第3の着信手段に蓄積される情報の処理とを行なう決済処理情報処理手段と、前記ユーザ情報処理手段、マーチャント情報処理手段及び決済処理情報処理手段との連携処理によってサービス提供処理におけるデータ処理を行なうサービスディレクタ情報処理手段とを具備することを特徴とする請求項4乃至6.1に記載のパーソナル電子決済システム。

【請求項63】 前記サービス提供手段の計算機システムが、前記ユーザ情報処理手段、マーチャント情報処理手段、決済処理機関情報処理手段及びサービスディレクタ情報処理手段の生成と消去とを制御するサービスマネージャ情報処理手段を具備し、前記ユーザ情報処理手段、マーチャント情報処理手段、決済処理機関情報処理手段、及びサービスディレクタ情報処理手段が、それぞれ必要に応じて、前記サービスマネージャ情報処理手段によって生成または消去されると特徴とする請求項62に記載のパーソナルサーバ装置の計算機システム。

【請求項64】 前記サービスマネージャ情報処理手段が、前記支払手段との通信のために、各支払手段のそれぞれに1対1で対応するユーザ情報処理手段を生成し、前記請求手段との通信のために、各請求手段のそれぞれに1対1で対応するユーザチャント情報処理手段を生成し、前記決済処理手段との通信のために、各決済処理手段のそれぞれに1対1で対応する決済処理情報処理手段を生成し、さらに、前記ユーザ情報処理手段、マージョント情報処理手段または決済処理情報処理手段の組み合わせで前記処理を行なうための情報処理手段を3つずつのサブシステムにそれぞれに対応させて1つのサブシステム3に統合し、それぞれに処理手段を生成することを特徴とする請求項63に記載のパーソナルネットワークシステム。

【請求項65】 前記サービスマネージャ情報処理手段が、前記サービスディレクタ情報処理手段を生成する際に、前記サービスディレクタ情報処理手段を含む、前記サービスディレクタ情報処理手段のグループを定義し、処理を行なうための情報処理手段のグループを定義し、生成された前記サービスディレクタ情報処理手段が、前記グループに属する情報処理手段と前記サービスマネージャ情報処理手段とのみ通信をして、前記サービスディレクタ情報処理手段との連携処理によって、サービス監視処理におけるデータ処理を行なうことを特徴とする情報処理システム63または64に記載のパーソナル電子決済システム4。

【請求項6】 前記サービスディレクトリ情報処理手段が、サービス提供処理におけるデータ処理を行う際に、自身が属する情報処理手段のグループに属さない他の情報処理手段と協働処理をする必要がある場合に、必要とする情報処理手段の前記グループへの追加を要求する。前記追加はサービスメタデータに要求されるサービスメタデータを生成して前記グループへ追加する。

ことを特徴とする請求項65に記載のパーソナル電子決済システム。

(請求項6) 前記ユーザ情報処理手段が、対応する支払手段と、自身が属するグループのサービスディレクタ情報処理手段と、サービスマネージャ情報処理手段とに著し、サービス提供手段の第1の蓄積手段に関する情報を前記支払手段及び前記支払手段の所有者に関する情報の処理を行ない、前記マニャント情報処理手段が、対応する請求手段と、自身が属するグループのサービスディレクタ情報処理手段と、サービスマネージャ情報処理手段とのみ通信をし、サービス提供手段に蓄積される前記請求手段の第2の蓄積手段に関する情報の処理を行ない、サービス提供手段と自身が属するグループのサービスディレクタ情報処理手段と、サービスマネージャ情報処理手段とのみ通信をし、サービス提供手段に蓄積される前記請求手段の第3の蓄積手段に関する情報の処理を行なうことを特徴とする請求項5

6 または6 に記載のパラメータ電子決済システム。

(請求項6) 前記支払手段と前記サービス提供手段を除く他の間で通信回線を接続する際に、前記支払手段とそれらに対応する前記ユーザ情報処理手段とが、相互の認証処理を行ない、前記請求手段と前記サービス提供手段とで通信回線を接続する際に、前記請求手段とそれにたいして、前記請求手段と前記サービス提供手段とが、相互の認証処理を行なうことを特徴とする請求項6乃至7に記載のパラメータ電子決済システム。

【請求項69】 前記支払手段、請求手段及び決済情報処理手段が、前記サービス提供手段の対応するユーザ情報処理手段、マーチャント情報処理手段または決済情報処理手段へ送附するメッセージングに、それぞれ、支払手段の所有者、請求手段の所有者または決済情報処理手段の所有者のデジタル署名を施し、また、前記ユーザ情報処理手段、マーチャント情報処理手段及び決済情報処理手段が、前記支払手段、請求手段または前記サービス提供手段の所有者のデジタル署名を施し、これらのデジタル署名が施されたメッセージングを受信した前記支払手段、請求手段、決済情報処理手段、マーチャント情報処理手段及び決済情報処理手段の各々が、前記デジタル署名の検証処理を行なうことを特徴とする請求項4乃至68に記載のバーコード決済システム。

【請求項70】前記支払手段、請求手段及び決済処理手段が、前記サービス提供手段の対応するユーザ情報処理手段に、マーチャント情報処理手段または決済処理手段を施し、情報処理手段に送信するメッセージデータに対して、前記サービス提供手段の所有者が対して封書化処理を施すこと、前記ユーザ情報処理手段、マーチャント情報処理手段及び決済処理手段が、前記支払手段、

請求手段または決済処理手段へ送附するメッセージデータに対して、前記支払手段、請求手段または決済処理手段の所有者若しくは封書化処理を施し、これらの封書化処理が施されたメッセージデータを受領した前記支払手段、請求手段、決済処理手段並びに前記サービス提供手段、ユーザ情報処理手段、マーケティング情報処理手段及び決済処理機関情報処理手段の各々が、封書化されたメッセージデータの暗号の復号化処理を行なうことを特徴とする請求項6乃至9に記載のパーソナル電子決済システム。

【請求項71】 前記支払手段、請求手段、決済処理手段及び前記サービス提供手段のユーザ情報処理手段、マERCHANT情報処理手段及び決済処理機関情報処理手段が、送信する前記メッセージにデジタル署名と、前記署名化処理とを併せて施し、前記メッセージデータを受取った前記支払手段、請求手段、決済処理手段並びに前記サービス提供手段のユーザ情報処理手段、マERCHANT情報処理手段及び決済処理機関情報処理手段の各々が、封書化したメッセージデータの暗号を復号化して、封書化したメッセージデータの内容を特定して、請求項70に記載のパーソナル電子決済システム。

**【請求項72】** 前記請求手段から決却処理を要求するメッセージデータを受信したマセチャータ情報処理手段が、決却処理を要求するメッセージを生成してサーバ端末に、決却じヤ情報処理手段へ送信し、前記支払手段から支払処理を要求するメッセージデータを受信したユーザ情報処理手段が、支払処理を要求するメッセージを生成し、

て前記サービスマネージャ情報処理手段へ送付し、メッセージに含まれる識別情報を基にこれらのメッセージを照合した前記サービスマネージャ情報処理手段が、サブシステムディレクトリ情報処理手段を生成して、前記サービスディレクトリ情報処理手段、ユーザ情報処理手段及びサービスディレクトリ情報処理手段からなる情報処理手段のグループウェアを定義し、前記サービスディレクトリ情報処理手段が、前記決裁処理を要求するメッセージと前記支払処理を要求するメッセージとの内容を照会して、決裁処理を実行する決裁処理手段を選択し、選択した決裁処理手段に対応する決裁処理情報処理手段の前記グループウェアの追加処理を前記サービスマネージャ情報処理手段に要求し、前記サービスマネージャ情報処理手段が、要求された決裁処理情報処理手段を生成して前記グループウェアを追加し、理研情報処理手段を生成して前記決裁処理情報処理手段に要求するメッセージを生成して前記決裁処理情報処理手段に要求するメッセージを送信する。

手段へ送償し、前記決裁処理機関情報処理手段が、このメッセージから、決裁処理を要求するメッセージデータを送信して、前記決裁処理手段へ送信し、前記決裁処理手段が、決裁処理の完了を表すメッセージを生成して前記サーバシステムに送信するとともに、前記決裁処理手段へ送償するとともに、前記決裁処理機関情報処理手段が、決裁処理の完了を表すメッセージを生成して前記サーバシステムに送信するとともに、前記決裁処理機関情報処理手段へ送償するものと、



完了を致すメッセージ、決裁処理の完了を致すメッセージ第3の番手手段に蓄積し、決裁処理の完了を致すメッセージ第3の番手を致した即ちビジネスプロセス情報処理手段が、決裁の完了を致すメッセージと文書の完了を致すメッセージとを生じ、それぞれ、前記一チャント情報処理手段と、前記二チャント情報処理手段へ送信し、前記二チャント情報処理手段が、受信したメッセージから、決裁の完了を致すメッセージと一チャントを生じて前記請求受理手段へ送信するとともに、前記決裁の完了を致すメッセージ、前記一チャント情報処理手段が、受信したメッセージに基づき、支払の完了を致すメッセージと一チャントを生じ、即ち支払手段へ送信するとともに、前記支払の完了を致すメッセージと一チャントを付与して前記請求第1の番手手段に蓄積することを特徴とする請求6乃至7に記載のバーチャル電子決済システム。

**【請求項 3】** 前記要求手段から該処理の取消処理を要求するメッセージを受信したチャート情報処理手段が、該処理の取消処理を要求するメッセージを生成してサブシステムへ情報処理手段へ送信し、前記支払手段から支払処理の取消処理を要求するメッセージを受信したユーザ情報処理手段が、該処理の取消処理を要求するメッセージを生成して前記サブシステムへ送信し、メッセージに含まれる識別情報を基にこれらのメッセージを照合した結果、前記サブシステムへ情報処理手段が、サブシステムレクタ情報処理手段を生成して、前記チャート情報処理手段、ユーザ情報処理手段及びサブシステムレクタ情報処理手段がなる情報処理手段のグループを定義し、前記サブシステムレクタ情報処理手段が、前記該処理の取消処理を要求するメッセージと前記支払処理の取消処理を実行した該処理取消処理手段とを特定した該処理取消手段に対応する該処理取消処理手段の前記サブシステムへの追加を前記サブシステムへ情報処理手段が、要求された該処理取消情報処理手段を生成して前記グループへ追加し、前記サブシステムレクタ情報処理手段が、該処理の取消処理を要求するメッセージを生成して、前記該処理取消情報処理手段へ送信し、前記該処理の取消処理を要求するメッセージとメッセージから、該処理取消情報処理手段が、該処理の取消処理を要求するメッセージとメッセージを生成して、前記該処理の完了を表すメッセージとメッセージを生成して、前記該処理取消情報処理手段が、該処理の完了を表すメッセージを生成して、前記該処理取消情報処理手段へ送信するとともに、前記該処理取消情報処理手段の完了を表すメッセージとメッセージを生成して、前記該処理の完了を表すメッセージを生成して、前記サブシステムの完了を表すメッセージを受信した前記サブシステム

イレクタ帳処理手段が、決裁者の取消処理の完了を遂行  
メッセージと支払の取消処理の完了を遂行メッセージと  
を生み出し、前記イーザ帳処理手段へ送信し、前記イー  
ザ帳処理手段が、受領したメッセージから、決済のす  
まわり情報処理手段が、受領したメッセージを生成して前記  
請求処理手段へ送達するとともに、前記決済の取消処理  
の完了を遂行メッセージをユーザ提供手段の第  
二の操作手段に寄附し、前記イーザ帳処理手段が、受  
領したメッセージから、支払の取消処理の完了を遂行メッ  
セージを生成して前記支払手段へ送達するとともに、前記  
支払の取消処理の完了を遂行メッセージをユーザ提供手  
段の第三の操作手段の第一の操作手段に寄附することと  
を特徴とする請求項6乃至12に記載のパーソナル電  
子決済システム。

【請求項 4】 前記請求手段が、決済の完了を送るメッセージの中から含まれる支払手段の所有者の識別情報を用いて、前記支払手段との通信を要求するメッセージを、データベースを生成して送信し、前記請求手段からデータベースを生成して送信したメッセージを受信したデータベース情報処理手段が、前記支払手段との通信を要求するメッセージを生成してデータベース情報処理手段へ送信し、前記データベース情報処理手段が、前記データベース情報処理手段とつながる情報処理手段のグループを定義し、前記データベース情報処理手段が、前記データベースに含まれる支払手段の所有者の識別情報に基いて対応する支払手段とその所有権を決定し、その特定した支払手段に対応するデータベース情報処理手段の前記グループへの追加を前記データベース情報処理手段が、要求し、前記データベース情報処理手段が、要求されたデータベース情報処理手段を生成し、前記グループへ追加した、前記データベース情報処理手段が生成している、前記支払手段の所有者が設定したアクセス制御情報を参照して、前記請求手段からのアクセスが禁止されていない場合に、前記請求手段との通信回線に接続し、前記データベースを生成して前記データベース情報処理手段へ送信し、前記データベース情報処理手段が、このメッセージから、前記請求手段との通信回線の接続を知らせるメッセージを生成して前記支払手段へ送信するメッセージを生成して前記データベース情報処理手段へ送信する請求項 6 4 に基づくデータベース電子決済システム。

【請求項76】 前記文法手段が、決断の完了を致すメッセージデータを生成して送信したとき、前記支払手段が前記メッセージデータを生成して送信するとき、前記支払手段との通信を要求するメッセージを受信し、前記決済手段との通信を要求するメッセージを受信してデータベース情報処理手段へ送信し、生成してデータベース情報処理手段へ送信し、生成してデータベース情報処理手段へ送信した前記データベース情報

理手段が、サーチ・ビズテック情報処理手段を生成し、前記サーチ・ビズテック情報処理手段と前記サーチ・ビズテック情報処理手段とからなる情報処理手段のグループを定義し、前記サーチ・ビズテック情報処理手段が、前記請求手段に示するサーチ・ビズテック情報処理手段の前置グループへの追加を前記サーチ・ビズテック情報処理手段に要求し、前記サーチ・ビズテック情報処理手段が、要求されたサーチ・ビズテック情報処理手段を生成し前記グループへ追加し、前記サーチ・ビズテック情報処理手段が、前記サーチ・ビズテック情報処理手段の追加を知らずして前記サーチ・ビズテック情報処理手段を生成し前記グループへ追加し、前記サーチ・ビズテック情報処理手段が、前記サーチ・ビズテック情報処理手段を生成し前記グループへ追加し、前記サーチ・ビズテック情報処理手段が、前記請求手段と前記請求手段へ送付するデータを生成して、前記請求手段へ送付することを特徴とする請求項6乃至7に記載のパーソナル電子装置。

【請求項 6】 前記決済手段または前記サービス提供手段が、前記支払手段または請求手段の第 2 のデータに基づくデータを更新要求するワンタッチデータに基づくされているデータの変更を要求するワンタッチデータを生成して前記支払手段または請求手段に送信した場合に、前記支払手段または請求手段の中央処理装置が、前記第 2 のデータに基づくされているデータを含むワンタッチデータを生成して前記決済手段または前記サービス提供手段に送信し、これを受けた前記決済手段または請求手段の第 2 のデータに基づくする更新データを含むワンタッチデータを生成して前記支払手段または請求手段の第 2 のデータに基づくする更新データを含むワンタッチデータを生成して前記決済手段の中央処理装置が、前記支払手段または請求手段または請求手段の更新データを含むワンタッチデータを生成して前記支払手段または請求手段に送信し、前記支払手段または請求手段の更新データを含むワンタッチデータから更新データを取り出して、第 2 のデータに基づくデータに基づくされているデータを更新することを特徴とする請求項 1乃至 7 に記載のパワー電子決済システム。

【請求項 7】 前記決済手段が、分散して配置された複数の決済手段によって構成され、それらの決済手段が、相互に接続によって相互に接続されていることを特徴とする請求項 1乃至 7 に記載のパワー電子決済システム。

【請求項78】 複数の前記決済手段が、地域ごとに、または、組織ごとに分散して配置されていることを特徴とする請求項77に記載のパーソナル電子決済システム。

【請求項 9】 前記支払手段及び支払手段の所有者に  
関する情報が、前記支払手段または支払手段の所有者と  
同じ属性を有する決済手段の第 1 の蓄積手段に蓄積され  
て、前記決済手段及び前記支払手段の所有者に関する情報  
が、前記請求手段または請求手段の所有者と同じ属性を  
有する決済手段の第 2 の蓄積手段に蓄積され、全ての決  
済手段の第 1 の蓄積手段には、さらに、その決済手段と  
該決済手段が持する全ての支払手段の識別情報と、前記決  
済手段及び支払手段の所有者に関する情報が蓄積されてい

いる場所を示す位置情報とが蓄積され、全ての決済手段の第2の蓄積手段には、さらに、その決済手段との通信が許される全ての請求手段の識別情報と、前記請求手段及び請求手段の所有者に関する情報が蓄積されているものも示す位置情報とが蓄積されていることを特徴とする請求項7または78に記載のパーソナル電子決済システム。

【請求項80】 前記サージス提供手段が、分散して配置された複数のサージス提供手段によって構成され、それらのサージス提供手段が通信回線によって相互に接続されていることを特徴とする請求項40乃至76に記載のパーソナル電子決済システム。

【請求項81】 複数の前記サービス提供手段が、地盤ごとに、または、組織ごとに分散して配置されていることを特徴とする請求項80に記載のパーソナル電子決済システム。

【請求項62】 前記文払手段及び文払手段の所有者に  
関する情報が、前記文払手段または文払手段の所有者と  
同じ属性を有するサブ・ビュ提供手段の第1の蓄積手段に  
蓄積され、前記請求手段及び積累手段の所有者に関する  
情報が、前記請求手段または積累手段の所有者と同じ属性  
を有するサブ・ビュ提供手段の第2の蓄積手段に蓄積され  
、全てのサブ・ビュ提供手段の第1の蓄積手段は、さ  
らに、そのサブ・ビュ提供手段との通信が可能な全ての  
文払手段の蓄積情報と、前記文払手段及び文払手段の所  
有者に関する情報が蓄積されている場所を示し属性情報  
とが蓄積され、全てのサブ・ビュ提供手段の第2の蓄積手  
段は、さらに、そのサブ・ビュ提供手段との通信が可  
能な全ての積累手段の蓄積情報と、前記請求手段及び積  
累手段の所有者に関する情報が蓄積されている場所を示  
す位置情報とが蓄積されていることを特徴とする請求項  
50または81に記述のパーソナル電子決済システム。

【請求項8 3】 前記風性が、「組織」であることを特徴とする請求項7または8 2に記載のパーソナル電子決済システム。

【請求項8 4】 前記風性が、「地域」であることを特徴とする請求項7または8 2に記載のパーソナル電子決済システム。

決済システム。  
【請求項85】 支払手段が、第2のサービ

と通信回線を接続し、前記第2のサーバへ入出力手段が、前記支払手段及び支払手段の所有者に関する情報を蓄積する第1のサーバへ入出力手段と出触する場合には、第2のサーバへ入出力手段のサーバとデータベース接続処理手段が、前記第2のサーバへ入出力手段の第1の接続手段に重複した手段の所有者情報と、前記支払手段及びび支払手段の所有者に関する情報が蓄積されている場所を示す位置情報とから、前記第1のサーバへ入出力手段を特定し、前記第1のサーバへ入出力手段のサーバとデータベース接続処理手段に前記支払手段に対するデータベース接続処理手段の生成を要求し、データベース接続処理手段

段が第1のサービス提供手段上生成された場合に、前配支支払手段に対処するモバイルユーザ情報処理手段を前配第2のサービス提供手段上生成し、生成された前配モバイルユーザ情報処理手段とホームユーザ情報処理手段とが、連携して、前配支払手段との間で、前配支払手段及び支払手段の所有者に関する情報の処理を行なうことを特徴とする請求項8乃至8 41に記載のパーソナル電子決済システム。

【請求項86】 支払手段が、第2のサービス提供手段のユーザ情報処理手段と通信回線を接続して、支払処理の取消処理を要求し、前記第2のサービス提供手段が、前記支払処理に関連した請求手段及びその所有者に関する情報を蓄積する第1のサービス提供手段と相連する場合に、第2のサービス提供手段のサービスマネージャ情報処理手段が、前記第2のサービス提供手段の第2の請求手段に蓄積されている請求手段の識別情報と、前記請求手段及び債権手段の所有者に関する情報が蓄積されてある場所を示す位置情報とから、前記第1のサービス提供手段を特定し、前記第1のサービス提供手段のサービスマネージャ情報処理手段に、前記ユーザ情報処理手段から受領した支払処理の取消を要求するメッセージを送信し、前記第1のサービス提供手段のサービスマネージャ情報処理手段が、前記第1のサービス提供手段のマーチャント情報処理手段から受領した決済処理の取消処理を要求するメッセージと、前記第2のサービス提供手段のユーザ情報処理手段に蓄積するメッセージとを照会して、第1のサービス提供手段上にサービスディレクタ情報処理手段を生成し、前記サービスディレクタ情報処理手段と前記マーチャント情報処理手段と前記第2のサービス提供手段のユーザ情報処理手段とから成る情報処理手段のグループを定義することを特徴とする請求項82乃至85に記載のバーチャル店舗システム。

【請求項8】 請求手段が、第2のサービス提供手段のマーチャント情報処理手段に支払手段との通信を要求するメッセージデータを送信し、前記第2のサービス提供手段が、前記支払手段及びその所有者に関する情報を保持する第1のサービス提供手段と相連する場合に、前記マーチャント情報処理手段から支払手段との通信を要求するメッセージを受信し、第2のサービス提供手段がサービスマネージャ情報処理手段が、第2のサービス提供手段にサービスディレクタ情報処理手段を生成し、前記マーチャント情報処理手段と前記サービスディレクタ情報処理手段とから成る情報処理手段のグループを定義し、生成された前記サービスディレクタ情報処理手段が、要求先の支払手段とその所有者とを特定し、特定した支払手段に対応するユーザ情報処理手段を前記グループへ追加する、よって前記サービスマネージャ情報処理手段に要求し、それを受けて前記サービスマネージャ情報処理手段が、前記第2のサービス提供手段の第1の

読み取り可能な形式で記録した処理プログラム記録媒体。

【請求項93】 請求項40乃至89に記載の前記サービス提供手段の計算機システムの処理プログラムを、電子計算機が読み取り可能な形式で記録した処理プログラム記憶媒体。

【請求項94】 請求項40乃至89に記載の前記決済処理手段の計算機システムの処理プログラムを、電子計算機が読み取り可能な形式で記録した処理プログラム記録媒体。

【発明の詳細な説明】

[0001]

【発明の属する技術分野】本発明は、クレジットカードカード（バンクカード）に代表される小売販売取引における決済機能を提供する電子決済システムに関し、特に、決済の安全性を担保し、円滑な決済処理を可能にするものである。

100021

【従来の技術】近年、クレジットカードに代表されるパ  
ンクカードの普及により、小売販売におけるクレジットカード  
カード決済は、一般的なものになっている。しかし、一  
方で、クレジットカードの偽造や、他人による不正使  
用、販売店による不正請求などのトラブルも増えてお  
り、決済システムとしての安全性の向上が求められている。  
最近では、クレジットカードの偽造防止対策の一つ  
として、ICカードタイプのクレジットカードも登場し  
てきている。

【0003】以下では、ICカードタイプのクレジットカードも含めた、従来のクレジットカードによる決済システムについて説明する。

【0004】従来、クレジットカードに代表されるパンクカードによる決済では、特公平3-32100号公報に開示されているように、販売店の端末とコントローラメントの間で、データ通信を行って、信用照会とクレジット決済を行なう決済システムが、数多く提案され、使用されている図42は、従来の一般的な決済システムの構成を示すものである。

【0005】図42において、クレジット決済増4201は、販売店に設置され、販売店でクレジット決済の操作を行なう端末である。クレジット決済増4201は、電話回線4204と、公衆網4203と、通信回線4205を介して、遠隔の決済システム4202に接続されている。クレジット決済増4201には、クレジットカード4200に格納されている情報を読み取るカードリーダーと、公衆網4203に接続するためのモデムと、計算書を印するプリンタとが備わっている。

【0006】決済システム4202は、クレジット決済処理を行なう情報処理システムであり、決済システム4202には、消費者とのクレジットサービスの契約の下に、消費者の信用情報と口座情報とが管理されている。

審判手段に審判されている支払手段の識別情報と、前記支払手段及び支払手段の所有者に関する情報が審判されている場所を示す位置情報とから、前記第1のサービス提供手段を特定し、前記第1のサービス提供手段のサービスマネージャ情報処理手段に前記支払手段に対応するユーザ情報処理手段の生成を要求し、第1のサービス提供手段上に支払手段に対応するユーザ情報処理手段が生じられた場合に、前記ユーザ情報処理手段を前記グループに追加することを特徴とする請求項8乃至86に記述のバーチャル電子決済システム。

【請求項 8】 支払手段が、第 2 のサービス提供手段のユーザ情報処理手段に請求手段との通信を要求するメッセージデータを送信し、前記第 2 のサービス提供手段が、前記請求手段及びその所有者に関する情報を蓄積する第 1 のサービス提供手段と相連する場合、前記ユーザ情報処理手段から請求手段との通信を要求するメッセージを受信した第 2 のサービスの提供手段のサービスマネージャ情報処理手段が、前記第 2 のサービスの提供手段の第 2 の蓄積手段に蓄積されている請求手段の識別情報と、前記請求手段及び請求手段の所有者に関する情報とを蓄積されている場所を示す位置情報とから、前記第 1 のサービスの提供手段を特定し、前記第 1 のサービスの提供手段のサービスマネージャ情報処理手段に、前記第 1 のサービスの提供手段から受信した、請求手段との通信を要求するメッセージを送信し、このメッセージを受信した前記第 1 のサービスの提供手段のサービスマネージャ情報処理手段が、第 1 のサービスの提供手段の上にサービスディレクトリ情報情報処理手段を生成して、前記サービスディレクトリ情報処理手段と前記第 2 のサービスの提供手段上のユーザ情報処理手段とから成る情報処理手段のグループを定義し、生成された前記サービスディレクトリ情報処理手段が、要求された請求手段に付するマーチャント情報処理手段を前記グループへ追加するように第 1 のサービスの提供手段のサービスマネージャ情報処理手段に要求し、それを受けて前記サービスマネージャ情報処理手段が、第 1 のサービスの提供手段上に前記請求手段に付するマーチャント情報処理手段を生成して、前記グループに追加するこの情報処理手段を生成して、前記グループに追加するこの手段と請求手段を、

【請求項8・9】 前記支払手段が、蓄積手段として、強誘電体メモリを具備することを特徴とする請求項1乃至8に記載のパーソナル電子決済システム。

【請求項 90】 請求項 5乃至 89 に記載の前記支払手  
段の中央処理装置の制御プログラムを、電子計算機が読  
み取り可能な形式で記録した制御プログラム記録媒体。  
【請求項 91】 請求項 6乃至 89 に記載の前記請求手  
段の中央処理装置の制御プログラムを、電子計算機が読  
み取り可能な形式で記録した制御プログラム記録媒体。  
【請求項 92】 請求項 7乃至 89 に記載の前記決済手  
段の計算機システムの処理プログラムを、電子計算機が  
読み取り可能な形式で記録した制御プログラム記録媒体。

読み取り可能な形式で記録した処理プログラム記録媒体。

【請求項93】 請求項40乃至89に記載の前記サービス提供手段の計算機システムの処理プログラムを、電子計算機が読み取り可能な形式で記録した処理プログラム記憶媒体。

【請求項94】 請求項40乃至89に記載の前記決済処理手段の計算機システムの処理プログラムを、電子計算機が読み取り可能な形式で記録した処理プログラム記録媒体。

【発明の詳細な説明】

**[0001]**

【発明の属する技術分野】本発明は、クレジットカードカード（バンクカード）に代表される小売販売取引における決済機能を提供する電子決済システムに関し、特に、決済の安全性を担保し、円滑な決済処理を可能にするものである。

100021

【従来の技術】近年、クレジットカードに代表されるパ  
ンクカードの普及により、小売販売におけるクレジットカード  
カード決済は、一般的なものになっている。しかし、一  
方で、クレジットカードの偽造や、他人による不正使  
用、販売店による不正請求などのトラブルも増えてお  
り、決済システムとしての安全性の向上が求められている。  
最近では、クレジットカードの偽造防止対策の一つ  
として、ICカードタイプのクレジットカードも登場し  
てきている。

【0003】以下では、ICカードタイプのクレジットカードも含めた、従来のクレジットカードによる決済システムについて説明する。

【0004】従来、クレジットカードに代表されるバン  
クカードによる決済では、特公平3-32100号公報  
に開示されているように、販売店の端末とコントローラ  
センタの間で、「データ決済」を行って、信用照会とクレ  
ジット決済を行なう決済システムが、数多く提案され、  
また、使用されている図42は、従来の一般的決済シ  
ステムの構成を示すものである。

【0005】図42において、クレジット決済増4201は、販売店に設置され、販売店でのクレジット決済の操作を行なう端末である。クレジット決済増4201は、電話回線4204と、公衆網4203と、通信回線4205を介して、遠隔の決済システム4202に接続されている。クレジット決済増4201には、クレジットカード4200に格納されている情報を読み取るカードリーダーと、公衆網4203に接続するためのモデムと、計算書を印するプリンタとが備わっている。

【0006】決済システム4202は、クレジット決済処理を行なう情報処理システムであり、決済システム4202には、消費者とのクレジットサービスの契約の下に、消費者の信用情報と口座情報とが管理されている。

審判手段に審判されている支払手段の識別情報と、前記支払手段及び支払手段の所有者に関する情報が審判されている場所を示す位置情報とから、前記第1のサービス提供手段を特定し、前記第1のサービス提供手段のサービスマネージャ情報処理手段に前記支払手段に対応するユーザ情報処理手段の生成を要求し、第1のサービス提供手段上に支払手段に対応するユーザ情報処理手段が生成された場合に、前記ユーザ情報処理手段を前記グループに追加することを特徴とする請求項8乃至86に記述のバーチャル電子決済システム。

【請求項 8】 支払手段が、第 2 のサービス提供手段のユーザ情報処理手段に請求手段との通信を要求するメッセージデータを送信し、前記第 2 のサービス提供手段が、前記請求手段及びその所有者に関する情報を蓄積する第 1 のサービス提供手段と相連する場合、前記ユーザ情報処理手段から請求手段との通信を要求するメッセージを受信した第 2 のサービスの提供手段のサービスマネージャ情報処理手段が、前記第 2 のサービスの提供手段の第 2 の蓄積手段に蓄積されている請求手段の識別情報と、前記請求手段及び請求手段の所有者に関する情報が蓄積されている場所を示す位置情報とから、前記第 1 のサービスの提供手段を特定し、前記第 1 のサービスの提供手段のサービスマネージャ情報処理手段に、前記第 1 のサービスの提供手段から受信した、請求手段との通信を要求するメッセージを送信し、このメッセージを受信した前記第 1 のサービスの提供手段のサービスマネージャ情報処理手段が、第 1 のサービスの提供手段の上にサービスディレクトリ情報が格納されている生成して、前記サービスディレクトリ情報処理手段と前記第 2 のサービスの提供手段上のユーザ情報処理手段と前記第 2 のサービスの提供手段上にサービスディレクトリ情報が格納されている生成して、前記サービスディレクトリ情報処理手段と前記第 2 のサービスの提供手段上のユーザ情報処理手段とから成る情報処理手段のグループを定義し、生成された前記サービスディレクトリ情報処理手段が、要求された請求手段に付するマーチャント情報処理手段を前記グループへ追加するように第 1 のサービスの提供手段のサービスマネージャ情報処理手段に要求し、それを受けて前記サービスマネージャ情報処理手段が、第 1 のサービスの提供手段上に前記請求手段に付するマーチャント情報処理手段を生成して、前記グループに追加する情報処理手段を生成して、前記グループに追加するものと被認とする請求項 8 乃至 7 に記載のパersoナルコンピュータシステム。

【請求項8・9】 前記支払手段が、蓄積手段として、強誘電体メモリを具備することを特徴とする請求項1乃至8に記載のパーソナル電子決済システム。

【請求項 90】 請求項 5乃至 89 に記載の前記支払手  
段の中央処理装置の制御プログラムを、電子計算機が読  
み取り可能な形式で記録した制御プログラム記録媒体。  
【請求項 91】 請求項 6乃至 89 に記載の前記請求手  
段の中央処理装置の制御プログラムを、電子計算機が読  
み取り可能な形式で記録した制御プログラム記録媒体。  
【請求項 92】 請求項 7乃至 89 に記載の前記決済手  
段の計算機システムの処理プログラムを、電子計算機が  
読み取り可能な形式で記録した制御プログラム記録媒体。

前段が第1のサービスピッチ提供手段上に生成された場合に、前配支払手段に対処するモバイルユーザー情報処理手段を前配第2のサービスピッチ提供手段上に生成し、生成された前配モバイルユーザー情報処理手段とホームページ情報処理手段とが、連携して、前配支払手段との間で、前配支払手段及び支払手段の所有者に関する情報の処理とを行なうことと特徴とする請求項8乃至8-4に記載のパーソナル電子決済システム。

【請求項86】 支払手段が、第2のサービス提供手段のユーザ情報処理手段と通信回線を接続して、支払処理の取消処理を要求し、前記第2のサービス提供手段が、前記支払処理に関連した請求手段及びその所有者に関する情報を蓄積する第1のサービス提供手段と相連する場合に、第2のサービス提供手段のサービスマネージャ情報処理手段が、前記第2のサービス提供手段の第2の請求手段に蓄積されている請求手段の識別情報と、前記請求手段及び債権手段の所有者に関する情報が蓄積されてある場所を示す位置情報とから、前記第1のサービス提供手段を特定し、前記第1のサービス提供手段のサービスマネージャ情報処理手段に、前記ユーザ情報処理手段から受領した支払処理の取消を要求するメッセージを送信し、前記第1のサービス提供手段のサービスマネージャ情報処理手段が、前記第1のサービス提供手段のマーチャント情報処理手段から受領した決済処理の取消処理を要求するメッセージと、前記第2のサービス提供手段のユーザ情報処理手段の取消処理を要求するメッセージとを照会して、第1のサービス提供手段上にサービスディレクタ情報処理手段を生成し、前記サービスディレクタ情報処理手段と前記マーチャント情報処理手段と前記第2のサービス提供手段のユーザ情報処理手段とから成る情報処理手段のグループを定義することを特徴とする請求項82乃至85に記載のバーチャル店舗システム。

【請求項8】 請求手段が、第2のサービス提供手段のマーチャント情報処理手段に支払手段との通信を要求するメッセージデータを送信し、前記第2のサービス提供手段が、前記支払手段及びその所有者に関する情報を保持する第1のサービス提供手段と相連する場合に、前記マーチャント情報処理手段から支払手段との通信を要求するメッセージを受信し、第2のサービス提供手段がサービスマネージャ情報処理手段が、第2のサービス提供手段上にサービスディレクタ情報処理手段を生成し、前記マーチャント情報処理手段と前記サービスディレクタ情報処理手段とから成る情報処理手段のグループを定義し、生成された前記サービスディレクタ情報処理手段が、要求先の支払手段とその所有者とを特定し、特定した支払手段に対応するユーザ情報処理手段を前記グループへ追加する、よって前記サービスマネージャ情報処理手段に要求し、それを受けて前記サービスマネージャ情報処理手段が、前記第2のサービス提供手段の第1の

るには、消費者は、何故ものカードを持ち歩く必要があり不便であった。

【0010】また、従来の決済システムでは、クレジットカードという物理的カードを照証の手段にしているため、一度クレジット決済を行った取引を、後でキャンセルするためには、消費者が、もう一度、取引をした、その場に行かなければならない不便さがあつた。

【0017】また、従来の決済システムでは、計算書を紙に印字する必要があるが、その印字時間が、販売の効率化のためには、ネックになっていた。また、一方で、クレジッタ決済のネット化は、フリントを装填する必要がある、このことが、クレジッタ決済網全体のコンバクト化と、コストダウンとのネックになっていた。

【0018】また、従来の決済システムでは、消費者に計算機にサインをしてもらう必要があり、店員が消費者にサインを依頼し、実際にサインをしてもらうまでにかかる時間が、クレジットカード決済にかかる時間の大部分を占めており、販売の効率化のネックになっていた。

【0019】本発明は、こうした従来の決済システムの課題を解決するもので、安全性と利便性とに優れた決済手段を提供することを目的としている。

**[0020]**

**【問題を解決するための手段】** そこで、本発明では、情報の系統の通信手段を具備する送次手段と、情報の系統の通信手段を具備する請求手段と、情報の系統の通信手段を具備する決済手段（または、情報の系統の通信手段を具備するサービース提供手段と、サービース提供手段との通信回線を具備する決済処理手段）とにより、パーソナルコンピュータシステムを構成している。この送次手段、請求手段及び決済手段（またはサービース提供手段と決済処理手段）の各々の間では、それぞれ異なる系統の通信手段を用いて通信が行なわれる。

〔0022〕この支払手段と決済手段（或は、以下「手段」として記述）との間の通信で決済情報と交換することにより、請求手段による不正な請求を防ぐことが、また、支払手段の識別情報や支払手段の所有者の識別情報が請求手段の担当者に知られることを防止できる。また、支払手段と請求手段との間で、必要情報の交換を通信手段で行なうことにより、販売の効率性を高めることができる。

**(0022)**

(貸倒の発生形態) 本説明の請求項1に記載の説明  
は、債権の集積の通付手段を具備する支払手段と、債権  
の集積の通付手段を具備する請求手段と、債権の集積の  
通付手段を具備する支払手段と、支払手段、請求手  
段及び支払手段の各々の間における通付を、それぞれす  
異なる集積の通付手段を用いて行なうようにしたものを  
いう。支払手段と請求手段との間の通付が請求情報をも  
つた、支払手段と請求手段との間の通付で支払情報を受  
けた、支払手段と請求手段との間の通付で支払情報を受

別情報や支払金額、取引の識別情報、それぞれのサイン（デジタル署名）を交換することにより、販売の効率化を図ることができる。

【0023】請求項2に記載の発明は、支払手段に、請求手段及び決済手段と通信する通信手段として、異なる種類の無線通信手段を設けたものであり、モバイル環境での利便性を向上させることができる。

10022 請求項3に記載の説明は、支払手段と請求手段との間の無償適值手段として、支払手段と決済手段との間の無償適值手段に比べて、適応可能な距離が短く、指向性が高い無償適值手段を適定したものであり、支払手段と請求手段との間の距離は高く、2メートルの範囲であるから、無償適值手段をこのように選択することによって、使用領域に適したシステム機能を取ることができ、

【0025】請求項4に記載の発明は、支払手段が請求手段と間の兼通通信手段として光通信手段を具備し、決済手段と間の兼通通信手段としてラジオ兼通通信手段を具備するものである。近距離の支払手段と請求手段との間では、赤外線などの光通信兼通通信手段を用いる。一方、遠距離の支払手段と決済手段との間では、ラジオ兼通通信手段を用いることにより、使用頻度に応じたシステム形態を取ることができ、

【0026】請求項5に記載の発明は、支払

入るべき手段と、光通信手段及び、光ファイバー光通信手段とを  
併用するべき光ファイバー光通信手段と、又は、金額の値を  
入力する入力手段と、光通信手段及び、光ファイバー光通信手段  
とによって送信されるデータの生成処理と光通信手段及び  
びファイバー光通信手段によって受信されたデータの処理  
とを行なう中央処理装置と、中央処理装置の動作を制御  
する制御プログラムを蓄積する第1の記憶手段と、中央  
処理装置によるデータの処理の結果を蓄積する第2の記憶  
手段と、中央処理装置によって処理されたデータを蓄積する  
第2の記憶手段とを兼ねたものであり、又は、民の所有する  
者による支払手段の操作と、支払手段が蓄積しているデータ  
の所有者への提示とが可能となり、支払手段の利便  
性を向上する。

【0022】請求項6に記載の発明は、請求手段1に、支払手段の側で通信を行なう光通信手段と、決済手段の側で通信を行なう通信手段と、請求する金額の値を入力力する入力手段と、光通信手段及び通信手段によって送受信されるデータの生成処理と光通信手段及び通信手段によって受信されるデータの処理とを行なう中央処理装置と、中央処理装置の動作を制御する制御プログラムを記憶する側の記憶手段と、中央処理装置によるデータを監視する側の監視手段と、中央処理装置によって生成されたデータを蓄積する第2の蓄積手段と、前記データのうち、担当者による請求手段の操作と、請求手段が蓄積したデータのうちデータの担当者への提示とが可能なデータと、請求手段の利便性が向上する。

【0028】請求項7に記載の発明は、決済手段に、支

私手段に関する情報を蓄積する第1の蓄積手段と、請求手段に関する情報を蓄積する第2の蓄積手段と、決裁処理におけるデータ処理を行なう計算機システムとを接続したものであり、**「文私手段及び請求手段から受信するデータに基づいて、決裁処理を実行する。」**

【0022】請求項8に記載の発明は、支払手段の中央処理機関が、支払手段の入力手段によって入力された値に相当する金額の支払処理を要求するによってサービス手段を生成して、決済手段に送信し、また、決済手段から受信した支払の完了を示すメッセージングを処理して、表示手段に出力し、さらに、処理したデータを支払手段の第2の通信手段に格納するように構成したものであり、支払手段の所有者が、口座、決済手段に対して、支払金額を指定して決済を求めることで、請求手段による不正利用を防ぐことができ、さらに、支払手段の所有者は支払の履歴（取引データ）を管理することができ、

【000303】請求項9に記載の発明は、支払手段の中央処理装置が、支払手段の入力手段によって入力された値に相当する金額の支払を申し出るメッセージングデータを作成して、請求手段に送信するように構成したものであり、支払手段の所有者が、直接、請求手段とは決済手段とに対して、支払う金額を指定して決済を行うことができる。請求手段による不正な請求を防ぐことができる。

中央銀行が、請求事項10に記載の発明は、請求手段の申請に相当する金額の支払を請求するようセーブシートを申し出るようセーブシートと、この支払を請求するようセーブシートとから、請求処理を要求するようセーブシートを生成して、請求手段に送信し、また、請求手段から受信した請求の完了を示すようセーブシートを受理して、請求手段の表示手段に出力し、さらに、受理したデータと請求手段の第2の表示手段に格納するように構成したものであり、請求手段半端では決済処理の要求メカニズムによる決済手段に送ることができないため、請求手段による不正請求が防止でき、また、請求手段の所有者は決済の履歴（取引データ）を管理することができ、

【0002】請求項1に記載の発明は、請求手段の中央処理装置が、支払手段を生成してジョータを生じ、支払手段の中央処理装置が、支払手段の中央処理装置と生じた支払手段を用いてジョータと、請求手段から受領した支払を請求するジョータとから支払処理を要求するジョータを生成して支払手段に送信し、決済手段が、請求手段から受領した決済処理を要求するジョータと支払手段から受領した支払処理を要求するジョータとを照合して決済処理を行なう手段に送信し、支払手段の完了を通知する手段に送信するように構成したものである。

あり、請求手段による不正請求と、支払手段による支払のごまかしとを防ぐことができる。

[0033] 請求項12に記述の通り、支払手段の中央処理装置が、請求手段に支払を申し出るメッセージングの中にそのメッセージングを識別する識別情報を入れ、また、決済手段に送る支払処理を要求するメッセージングの中に、支払を申し出るメッセージングの識別情報と、支払手段に支払を請求するメッセージングの中にそのメッセージングを識別する識別情報を入れ、また、決済手段に送る決済情報を要求するメッセージングの中に、支払を請求するメッセージングの識別情報と、請求手段の識別情報と；支払を申し出るメッセージングの識別情報と；支払を申し出るメッセージングの識別情報とを入れ、決済手段が、支払処理を要求するメッセージングに決済手段の識別情報と支払いメッセージングの識別情報とを照合するように構成したものであり、請求手段の所有者の公的な識別情報、あるいは、支払手段を行なうことができ、カレジャトカーは野に相当する、識別情報の漏洩を防ぐことができる。

【0034】請求項13に記述の発明は、支払手段の第2の支払手段には、複数の支払方法の識別情報が格納され、支払手段の中央処理装置は、支払手段の入力手段によって選択された支払方法の識別情報と、支払を申し出るユーザに渡された支払方法を請求する、一つのジェータの中に、これらによって構成したものであり、一つの支払手段で、複数の支払方法の中から、支払方法を適宜選択することができる。そのため、何故ものとしてソフトカーを必要とせず、支払手段の所有者の利便性が向上する。

【0033】請求項14に記述の発明は、決済手段が、別決済手段の所有者に対して、決済の完了を通知する決済手段の所有者に、決済手段の所有権やその所有権の移転を主張して、決済の完了を通知するよう構成したものである。別決済手段に対して、支払手段の決済情報やその所有権の公的識別情報は一切開示されず、決済手段でその所有者の公的識別情報を考慮して決済手段が生じ、支払手段の所有者の識別情報だけが知られる。

【0036】請求項15に記述の発明は、支払手段が、支払手段のネットワーク一寄越に出張する支払い端末が、出張先で出張し、ネットワークを介してQ（Q>0）以下に上乗せした手数料を支払うことを特徴とする。中央処理装置になったとき、支払手段の中央処理装置が、中央処理装置の通知したデータが蓄積されている支払手段の第2の蓄積手段のデータを決済手段に送信し、決済手段が、受信したデータを、支払手段に関する情報を保持する決済手段の第1の蓄積手段に蓄積すると同時に前記のものである。また、ネットワークによって、支払手段が蓄積されてい



(17)

となり、支払手段の所有者は、取引をしようとする相手と合意することができ、円滑に商取引を行なうことができる。

【0054】請求項33に記載の発明は、前記請求手段に、音声入力手段と、音声出力手段と、音声入力手段から入力される音声データと通信手段で送信されたデータへ変換し、且つ、通信手段で受信されたデータを音声出力手段によって出力される音声データへ変換する音声データ処理手段とを設けたものであり、音声データ通信が可能となり、請求手段の近接者は、お昼さんと合意をすることができ、円滑に商取引を行なうことができる。

【0055】請求項34に記載の発明は、前記支払手段に、送信するメッセージデータの暗号化処理と受信したメッセージデータの暗号の復号化処理とを行なう暗号処理手段と、送信する音声データの暗号化処理と受信した音声データの暗号の復号化処理とを行なう音声暗号処理手段とを設けたものであり、メッセージデータと音声データとを暗号化して送受信することが可能となり、取引の安全性が向上し、しかも、盗聴などから業務上の秘密を守ることができる。

【0056】請求項35に記載の発明は、請求手段に、送信するメッセージデータの暗号化処理と受信したメッセージデータの暗号の復号化処理とを行なう暗号処理手段と、送信する音声データの暗号化処理と受信した音声データの暗号の復号化処理とを行なう音声暗号処理手段とを設けたものであり、メッセージデータと音声データとを暗号化して送受信することが可能となり、取引の安全性が向上し、しかも、盗聴などから業務上の秘密を守ることができる。

【0057】請求項36に記載の発明は、支払手段が、支払手段の所有者のデジタル署名を施し、さらに、決済手段の所有者に対して封鎖化処理を施したメッセージデータを、決済手段へ送信するようにしたものであり、支払手段の所有者に成りすました不正な支払を防止でき、しかも、プライバシーを守ることができ。

【0058】請求項37に記載の発明は、請求手段が、決済手段へ送信するメッセージデータに、決済手段の所有者のデジタル署名を施すとともに、決済手段の所有者に対して封鎖化処理を施すようにしたものであり、請求手段の所有者に成りすました不正な請求を防止でき、しかも、取引の秘密を守ることができ。

【0059】請求項38に記載の発明は、決済手段が、支払手段へ送信するメッセージデータに、決済手段の所有者のデジタル署名を施すとともに、支払手段の所有者に対して封鎖化処理を施し、また、請求手段へ送信するメッセージデータに、決済手段の所有者のデジタル署名を施すとともに、請求手段の所有者に対して封鎖化処理を施すようにしたものであり、決済手段の所有者に成りすました不正な決済処理を防止でき、しかも、商取引の秘密を守ることができ。

(18)

手段が、請求手段に送信した決済の完了を返すメッセージデータをサージス提供手段の第2の蓄積手段に蓄積し、支払手段に送信した支払の完了を返すメッセージデータをサージス提供手段の第1の蓄積手段に蓄積するようにしたものであり、これによって、例えば、支払手段または請求手段が故障して、内部のデータが失われても、決済手段の第1の蓄積手段または第2の蓄積手段に蓄積されたメッセージデータをもとに、失われたデータを復旧することができ。

【0066】請求項45に記載の発明は、決済処理手段と、取り扱う決済処理の権限を異にする複数の決済処理手段によって構成し、サージス提供手段に、決済処理手段に関する情報を蓄積する第3の蓄積手段を設けたものであり、支払手段の所有者は、複数の支払方法を使用することが可能となり、支払手段の利便性が向上する。請求項46に記載の発明は、サージス提供手段が、決済処理を要求するメッセージデータと支払処理を要求するメッセージデータを送る送受信手段を、複数の決済処理手段の中から選択するようにしたものであり、決済処理を要求するメッセージデータの内容と、支払処理を要求するメッセージデータの内容と、最適な決済処理手段を選択することができ。

【0067】請求項47に記載の発明は、サージス提供手段が、決済処理手段から受信した決済処理の完了を返すメッセージデータを、サージス提供手段の第3の蓄積手段に蓄積するようにしたものであり、決済処理の完了を返すサージスデータと、決済の完了を返すメッセージデータと、支払の完了を返すメッセージデータと、支払いの整合性を保って蓄積管理でき、システムの信頼性が向上する。

【0068】請求項48に記載の発明は、サージス提供手段の第1の蓄積手段に蓄積される支払手段の所有者に関する情報の中に、支払手段の所有者の決済処理契約に関する情報と、支払手段の所有者に帰属する情報とが含まれ、サージス提供手段の第2の蓄積手段に蓄積される請求手段の所有者に関する情報の中に、請求手段の所有者の決済処理契約に関する情報と、請求手段の所有者に帰属する情報とが含まれるようにしたものであり、サージス提供手段は、サージス提供手段の第1の蓄積手段に蓄積された情報に基づいて、支払手段の所有者の認証と、請求手段の所有者に対する支払手段の所有者の証明とをすることが可能となり、また、サージス提供手段の第2の蓄積手段に蓄積された情報に基づいて、請求手段の所有者の認証と、支払手段の所有者に対する請求手段の所有者の証明とをすることが可能となり、支払手段の所有者と請求手段の所有者との間で、円滑に商取引を行なうことができる。

【0069】請求項49に記載の発明は、サージス提供手段の第1の蓄積手段の情報が、支払手段の所有者ごと

に管理して蓄積され、サージス提供手段の第2の蓄積手段の情報が、請求手段の所有者ごとに管理して蓄積されるようにしたものであり、決済に伴う個人のプライバシーに関する情報を、安全に、しかも、効率的に管理できることが可能となり、システムの信頼性が向上する。

【0070】請求項50に記載の発明は、支払手段の中央処理装置が、支払を申し出るメッセージデータ及び支払処理を要求するメッセージデータの中に、そのメッセージデータの有効期間情報を入れ、請求手段の中央処理装置が、支払を請求するメッセージデータ及び決済処理を要求するメッセージデータの中に、そのメッセージデータの有効期間情報を入れ、決済手段またはサージス提供手段が、支払処理を要求するメッセージデータと決済処理を要求するメッセージデータとを照合する際に、有効期間情報を照合するようにしたものであり、古いメッセージデータを出力した、不正な要求を防止することができる。

【0071】請求項51に記載の発明は、請求手段の中央処理装置が、決済処理を要求するメッセージデータを生成する前に、支払手段の所有者の照会処理を要求するメッセージデータを生成してサージス提供手段へ送信し、サージス提供手段が、支払処理を要求するメッセージデータと照会処理を要求するメッセージデータとを照合して、サージス提供手段の第1の蓄積手段に蓄積された支払手段の所有者に関する情報から、所有者の照会結果を示すメッセージデータを生成して請求手段へ送信し、請求手段の中央処理装置が、このメッセージデータを照合して、請求手段の表示手段に出力するようにしたものであり、請求手段の所有者は、支払手段の所有者の信用状況や、本人確認をしてから、決済処理を行なうことができる。商取引の安全性が向上する。

【0072】請求項52に記載の発明は、サージス提供手段の第1の蓄積手段に蓄積される支払手段の所有者に関する情報の中に、支払手段の所有者の写真情報と年齢情報とが含まれ、サージス提供手段が、所定の照会結果を示すメッセージデータの中に、支払手段の所有者の写真情報と年齢情報とを含めるようにしたものであり、請求手段の所有者は、請求手段の表示手段に出力された顔写真や年齢をもとに、支払手段の所有者の本人確認を行なうことができ、商取引の安全性が向上する。

【0073】請求項53に記載の発明は、支払手段の第2の蓄積手段の空率率量AAU (AAU>0) 未満になった場合に、支払手段の中央処理装置が、支払手段の第2の蓄積手段に蓄積されているデータを決済手段またはサージス提供手段に送信し、決済手段またはサージス提供手段から更新データを受信して、第2の蓄積手段に蓄積されているデータを更新するようにしたものであり、支払手段の第2の蓄積手段のデータが溢れるのを防止できる。

【0074】請求項54に記載の発明は、請求手段の第

2の落着手段の空き容量がN (AN>0)未満になった場合には、請求手段の中央処理装置が、請求手段の第2の落着手段に蓄積されているデータを落着手段またはサービス提供手段に返却し、次に落着手段またはサービス提供手段から更新データを受領して、第2の落着手段に蓄積されているデータを更新するようにしたものであり、請求手段の第2の落着手段のデータが溢れるのを防止でき

【0075】請求項55に記載の発明は、支払手段から支払手段の第2の清償手段に蓄積されているデータを含むメッセージデータを受信した。決済手段またはサーバと通信する手段が、支払手段の第2の蓄積手段の更新プログラムと新しい支払手段の中央処理装置の制御プログラムとを含むメッセージデータを生成して支払手段に送信し、そのメッセージデータを受領した。支払手段の中央処理装置が、新しい支払手段の中央処理装置の制御プログラムを、支払手段の第1の蓄積手段または第2の蓄積手段に蓄積して、その制御プログラムを実行するようにしたものであり、所有者の手をわずらわすことなく、支払手段の制御プログラムを、常に、最新バージョンに更新し、また、決済手段、あるいは、サービス提供手段も、支払手段の制御プログラムのバージョンの違いに対応する必要がある。

【0076】請求項56に記載の発明は、請求手段から請求手段の第2の蓄積手段に蓄積されているデータを含むメッセージデータを受信した、決済手段またはサーバと新しい請求手段の第2の蓄積手段の更新プログラムとを含む請求手段の中央処理装置の制御プログラムとを、そのメッセージデータを生成して請求手段に送信し、そのメッセージデータを受信した、請求手段の中央処理装置が、新しい請求手段の中央処理装置の制御プログラムを、請求手段の第1の蓄積手段または第2の蓄積手段に蓄積して、その制御プログラムを実行するようにしたものであり、所有者の手をわずらわずことなく、請求手段の制御プログラムを、常に、最新バージョンに更新でき、また、決済手段、あるいは、サーバに提供手段も、請求手段の制御プログラムのバージョンの違いに対応する必要がある。

【0077】請求項57に記載の発明は、決済手段またはサービス提供手段が、決済の完了を教示メッセージ、データ及び支払の完了を教示メッセージの中に、決済処理の識別情報を入れ、支払手段及び請求手段の中央処理装置が、支払処理または決済処理の取消処理を要求する際に、決済手段またはサービス提供手段が、支払手段及び請求手段のそれぞれから受信した支払処理及び決済処理の取消処理を要求する各メッセージを、決済処理の識別情報と照合するようにしているものであり、決済処理の識別情報と照合することによって、不正な取消処理の要求を防止できる。

【0078】請求項58に記載の発明は、サービス提供した手段が、支払手段及び請求手段のそれぞれから受信した支払処理及び決済処理の取消処理を要求するメッセージデータを照会する際に、さらに、支払処理の取消処理を要求するメッセージデータとサービス提供手段の第1の蓄積手段に蓄積されている支払の完了を教すメッセージデータの蓄積手段に蓄積されている支払の完了を教すメッセージデータの照会を行なうにしたものであり、支払処理の取消処理を要求するメッセージデータとサービス提供手段の第2の蓄積手段に蓄積されている決済の完了を教すメッセージデータとの照会と、決済処理の取消処理を要求するメッセージデータとサービス提供手段の第2の蓄積手段に蓄積されている決済の完了を教すメッセージデータとの照会によって、不正な取消処理の要求を防止できる。請求項59に記載の発明は、サービス提供手段が、請求項58に記載した決済処理の完了を教すメッセージデータをサービス提供手段の第2の蓄積手段に蓄積し、支払手段に送信した支払処理の取消処理の完了を教すメッセージデータをサービス提供手段の第1完了を教すメッセージデータとサービス提供手段の第1の蓄積手段に蓄積するようにしたものであり、これによって、例えば、支払手段または請求手段が故障して、内庫のデータが失われたとき、請求手段の第1の蓄積手段または第2の蓄積手段に蓄積されたメッセージデータをともに失われたデータを確認することができ、

【0079】請求項60に記載の発明は、決済手段またはサービス提供手段によって通信回線を接続された支払手段と請求手段とが、音声データ通信を行なうようにしたものであり、支払手段の所有者と請求手段の所有者とは、会話をすることができ、円滑に商取引を行なうことができる。

【10080】請求項61に記載の発明は、決済手段またはサービス提供手段によって通信回線を接続された支払手段と請求手段とが、暗号鍵を交換して、互いに音声データを暗号化して音声データ通信を行なうようにしたものである。支払い手段の所有者と請求手段の所有者は、お互いの会話が盗聴されることなく、円滑に暗号化を行なうことができる。

【0081】請求項62に記載の発明は、サーバ提供手段の計算機システムに、支払手段との通信とサーバ提供手段の第1の蓄積手段に蓄積される情報の処理とを行なうユーザ情報処理手段と、請求手段との通信とサーバ提供手段の第2の蓄積手段に蓄積される情報の処理とを行なうマーチャント情報処理手段と、決済処理手段との通信とサーバ提供手段の第3の蓄積手段に蓄積される情報の処理とを行なう決済処理情報処理手段と、ユーザ情報処理手段と、マーチャント情報処理手段及び決済処理情報処理手段との連携処理によってサーバ提供処理におけるデータ処理を行なうサーバ提供ディ

レクタ情報処理手段とを駆使したものであり、ユーザ情報処理手段とマシント情報処理手段とが連携して情報処理手段とサービスディレクタ情報処理手段とで、並列処理を行なうことによって、効率的にサービス提供処理を行なうことが出来る。

【0082】請求項63に記載の発明は、サービス提供手段の計算機システムに、ユーザ情報処理手段、マーケティング情報処理手段、決済処理関連情報処理手段及びサービスディレクタ情報処理手段の生成と消去とを制御するサービスマネージャ情報処理手段を設け、ユーザ情報処理手段、マーケティング情報処理手段、決済処理関連情報処理手段及びサービスディレクタ情報処理手段が、それぞれ必要に応じて、サービスマネージャ情報処理手段により生成または消去されるようにしたものであり、計算機システムの計算機能を、各情報処理手段に対して、効果的に配分することができ、

【0083】請求項64に記載の発明は、サービスマネージャ情報処理手段が、支払手段との通信のために、各支払手段のそれぞれに1対1で対応するユーザ情報処理手段を生成し、請求手段との通信のために、各請求処理手段のそれぞれに1対1で対応するチャータン情報処理手段を生成し、決裁処理手段との通信のために、各決裁処理手段を生成し、決裁処理手段に1対1で対応する決裁処理情報処理手段、ユーザ情報処理手段、マーケティング情報処理手段または決裁処理情報処理手段が連携処理を行なうための情報処理手段の組み合わせのそれぞれに対応させて1つずつのサービスディレクタ情報処理手段を生成するようにしたものであり、同時に、各情報処理手段を生成することができ、また、各情報処理手段を提供処理を行なうことができるので、メンバ情報処理手段の処理を単純化することができると、メンテナンスが容易となり、システムの信頼性を向上させることができる。

【0084】請求項65に記載の発明は、サーバシステム  
ーザ情報処理手段が、サーバシステム情報処理手段を  
生成する際に、サーバシステム情報処理手段を含む  
含む、連携処理を行なうための情報処理手段のグルー  
を定義し、生成されたサーバシステム情報処理手段  
が、グループに属する情報処理手段とのみ連携をして、  
グループに属する情報処理手段との連携処理によって、  
サーバシステム提供処理におけるデータ処理を行なうようにし  
たものであり、1つの情報処理手段のグループの処理  
たものであり、1つの情報処理手段のグループの処理  
たものであり、1つの情報処理手段のグループの処理  
たものであり、1つの情報処理手段のグループの処理

【0085】請求項66に記載の発明は、サービスディレクトリ情報処理手段が、サービス提供処理におけるデータ処理を行なう際に、自身が属する情報処理手段のグループに属さない情報処理手段と連携処理をする必要が生ずる場合に、必要とする情報処理手段のグループへの参加を要求するメッセージをサービスマネージャ情報処理手段へ送信し、サービスマネージャ情報処理手段が、要

された情報処理手段を生成してグループへ追加するよう  
にしたものであり、情報処理手段のグループの連携処理  
の途中で、新たな情報処理手段を追加できるので、自由  
度の高いサービス提供処理を行なうことができる。

【0088】請求項67に記載の発明は、ユーザ情報処理手段が、対応する支払手段と、自身が属するグループのサービスマネージャ情報処理手段と、サービスマネージャ情報処理手段ととのみ通信を行い、サービス提供手段の第1の審判処理手段に審判される支払手段及び支払手段の所有者に関する情報の処理を行ない、マーチャント情報処理手段が、対応する請求手段と、自身が属するグループのサービスマネージャ情報処理手段と、サービスマネージャ情報処理手段とのみ通信を行い、サービス提供手段の第2の審判処理手段に審判される請求手段及び請求手段の所有者に関する情報の処理を行ない、決済処理機関情報処理手段が、対応する決済処理手段と、自身が属するグループのサービスマネージャ情報処理手段と、サービスマネージャ情報処理手段とのみ通信を行い、サービス提供手段の第3の審判処理手段に審判される決済処理手段に関する情報の処理を行なうようにしたものであり、1つの情報処理手段のグループの処理が、他の情報処理手段に影響を与えないことなく、また、1つの情報処理手段（ユーザ情報処理手段、マーチャント情報処理手段、決済処理機関情報処理手段）の処理が、その情報処理手段に1対1に対応する対象（支払手段、請求手段、決済処理機関）に属さない情報処理手段を処理することなく、システムの情報性が向上する。

【0087】請求項68に記載の発明は、支払手段とサービス提供手段との間で通信回線を接続する際に、支払手段とそれとに対応するユーザ情報処理手段とが、相互の通信処理を行ない、請求手段とサービス提供手段との間で通信回線を接続する際に、請求手段とそれとに対応するマーチャント情報処理手段とが、相互の通信処理を行なうようにしたものであり、不正な取扱いを防止し、相手手に接続し、相手側の情報を不正に読み出したとき、情報を検知したりすることを防止できる。

【0088】請求項69に記載の発明は、支払手段、請求手段及び決済処理手段が、サービス提供手段に対応するユーザ情報処理手段、マーチャント情報処理手段または決済処理機側情報処理手段へ送附するメッセージデータに、それぞれ、支払手段の所有者、請求手段の所有者、または決済処理手段の所有者のデジタル署名を施し、また、ユーザ情報処理手段、マーチャント情報処理手段及び決済処理機側情報処理手段が、支払手段、請求手段または決済処理手段へ送附するメッセージデータにサービス提供手段のデジタル署名を施し、これらのデジタル署名が施されたメッセージデータを受信した支払手段、請求手段、決済処理手段並びにサービス提供手段のユーザ情報、決済処理手段、マーチャント情報処理手段及び決済処理機側情報処理手段の各々が、デジタル署名の検証処理を遂行する。



行なうようにしたものであり、成りすましてによる、不正な操作を防止することができ、また、サービスマン提供手段は、メニュー・プログラミにデジタル署名を施す処理とデジタル署名の検証処理とを、ユーザ情報取得手段とマニピュレーション取得手段とをそれぞれ別個の処理手段とがそれぞれ並列に処理することによって、効率的に行うことが可能である。

【0089】請求項70に記載の発明は、支払手段、請求手段及び決済処理手段が、サービス提供手段の対応するユーザ情報処理手段、サービス提供者情報処理手段または決済処理機関付情報処理手段に送達するメッセージデータに対して、サービス提供手段の所有者若しくは管理を施し、また、ユーザ情報処理手段、サービス提供者情報処理手段及び決済処理手段が、サービス提供者情報処理手段または決済処理手段へ送達するメッセージデータに対して、支払手段、請求手段または決済処理手段の所有者若しくは管理に付随して、これらの封装化処理が施されたメッセージデータを受領した支払手段、請求手段、決済処理手段並びにサービス提供手段のユーザ情報処理手段、サービス提供者情報処理手段及び決済処理機関付情報処理手段の各々が、封装化されたメッセージデータの暗号の復号化処理を行なうようにしてあり、

該暗号は、前記面図における状態を示すことができ、また、サービス提供手段は、メッセージデータの封装化処理と管理に付随したメッセージデータの暗号復号化処理とをユーザ情報処理手段とサービス提供者情報処理手段と決済処理機関付情報処理手段とが、それぞれ並列に処理することによって、効率的に行うことができる。

【0069】請求項71に記載の発明は、支払手段、請求手段、決済処理手段並びにサービス提供手段のユーザ情報情報処理手段、ユーザデータ情報処理手段及び決済処理手段が、送信するメッセージデータにデジタル署名を付与し、デジタル署名を併せて施し、メッセージデータを受信した支払手段、請求手段、決済処理手段及び決済処理手段は、ユーザデータ情報処理手段のユーザ情報処理手段、ユーザデータ情報処理手段及び決済処理手段が、ユーザデータ情報処理手段及び決済処理手段のユーザ情報処理手段の各々が、おこなったメッセージデータの署名を復号化して、デジタル署名の検証処理を行なうようにしたのである。このように、前記取扱いにおけるおこなうことが、同時に、成立することによる、不正な操作を防止でき、また、サービス提供手段は、送信するメッセージデータのデジタル署名を付与したデジタル署名の検証処理とを兼ねて行なうことができる。

【0099】請求項72に記載の発明は、請求手段が、  
 決裁処理を要求するメッセージングを受信したマニファ  
 シェン情報処理手段が、決裁処理を要求するメッセ  
 ージを送信してサーバにスプーン情報処理手段へ送信し  
 て、支払手段が支払処理を要求するメッセージングを  
 送信したユーザ情報処理手段が、支払処理を要求するメ

セージを生成してサードスタンダード情報処理手段へ送信し、メッセージに含まれる識別情報に基づいてこのメッセージを照会したサードスタンダード情報処理手段が、サードスタンダード情報処理手段を生成して、データベース情報処理手段、ユーザ情報処理手段及びサードスタンダード情報処理手段からなる情報処理手段のグループを定義し、サードスタンダード情報処理手段が、決裁処理を要求するメッセージと支払処理を要求するメッセージとの内容を確認して、決裁処理を実行する決裁処理手段を通知し、通知した決裁処理手段に対応する決裁処理手段を通知し、照会した決裁処理手段は、サードスタンダード情報処理手段のグループの追加をサードスタン

[illegible]

引における故障処理や成りすましてによる不正操作に際する  
 (10092) 補足項73に記載の表明は、請求手帳から以下の  
 法廷処理の取扱いを要求するメッセージングを受信した  
 デバイスに、情報処理手段が、法廷処理の取扱いを要  
 求するメッセージを生成してデバイスにメッセージング  
 情報処理手段へ送信し、支払手段から支払処理の取扱い  
 を要求するメッセージングを受信したユーザ情報処理  
 手段が、支払処理の取扱いを要求するメッセージを生  
 成してデバイスにメッセージング情報処理手段へ送信し、メ  
 セージに含まれる識別情報を基にこれらのメッセージを  
 照合したデバイスにメッセージング情報処理手段及びバ  
 イスにメッセージング情報処理手段及びデバイスにメ  
 ッセージング情報処理手段、ユーザ情報処理手段及びバ

鑑み、処理を要するメッセージと本処理の取消処理を  
 要求するメッセージとの内容を照合して、該処理を実行  
 した該処理手段と特定し、特定された該処理手段の  
 宛先とする該処理機関情報処理手段のグループへの追加  
 をサービスベンダ・ソフトウェア情報処理手段に要求し、サ  
 ービスベンダ・ソフトウェア情報処理手段が、該処理機  
 関情報処理手段を生成してグループへ追加し、サービス  
 ベンダ・ソフトウェア情報処理手段が、該処理機関情報  
 処理手段の生成して該処理機関情報処理手段へ送信し  
 ら、該処理機関情報処理手段を要求するメッセージか  
 ら、該処理機関情報処理手段を生成して、該処理機  
 関情報処理手段へ送付し、該処理機関情報処理手段が

されらる。決済処理画面情報処理手段が、決済処理の取消処理の完了を致すメッセージを生成してサージングデータの情報処理手段へ送信するとともに、決済処理の取消処理の完了を致すメッセージをサージング提供手段の第3の蓄積手段に蓄積し、決済処理の取消処理の完了を致すメッセージを受信したサージングクライアント情報処理手段が、決済の取消処理の完了を致すメッセージと支払の取消処理の完了を致すメッセージを生成して、それぞれ、サージング情報処理手段と、サージング情報処理手段とへ送信し、サージング情報処理手段が、受信したメッセージから、決済の取消処理の完了を致すメッセージデータを生じして請求処理手段へ送信するとともに、決済の取消処理の完了を致すメッセージデータをサージング提供手段の第2の蓄積手段に蓄積し、ユーザ情報処理手段が、受信したメッセージから、支払の取消処理の完了を致すメッセージデータの完了を致すメッセージデータを生じして支払手段へ送信するとともに、支払の取消処理の完了を致すメッセージデータをサージング提供手段の第1の蓄積手段に蓄積するようにした。よって不正操作を防止しながら、効率的にキャンセル処理が行なわれる。

注述の完了まで、各メンバーがメンバーシップのうちに含まれる支払手段の所有者の識別情報を用いて、支払手段と通信を要求するメッセージングデータを生成して送信した。請求手段からこのメッセージングデータを受信したメンバーシップ情報処理手段が、支払手段との通信を要求するメッセージを生成してサーバーメンバーシップ情報処理手段へ送信し、このメッセージを受信したサーバーメンバーシップ情報処理手段が、サーバーメンバーシップ情報処理手段を生成して、メンバーシップ情報処理手段とサーバーメンバーシップ情報処理手段とを有する情報処理手段のグループを定義し、サーバーメンバーシップ情報処理手段が、メッセージに含まれる支払手段の所有者の識別情報に対する応答を生成し、支払手段とその所有者とを特定し、その特定した支払手段による

送る。効率的に顧客サービスコールの処理を行なうことが出来る。

【0099】請求項75に記載の発明は、支払手段が決済の完了を教すメッセージ—ジデータを出力して、請求手段が該メッセージを受信し—ジデータを生成して送信したとき、支払手段からメッセージ—ジデータを受信したユーザ情報処理手段が、請求手段との通信回路を要求するメッセージを生成してサビスデータ—ジ情報処理手段へ送信し、このメッセージを受信したサビスデータ—ジ情報処理手段が、サビスデータ—ジ情報処理手段を生成して、ユーザ情報処理手段とサビスデータ—ジ情報処理手段とを有する情報処理手段のグループを定義し、サビスデータ—ジ情報処理手段が、請求手段に示すサビスデータ—ジ情報処理手段のグループへの追加サビスデータ—ジ情報処理手段が、要求されたサビスデータ—ジ情報処理手段を生成してグループへ追加し、サビスデータ—ジ情報処理手段が、支払手段との通信回路の接続を知らせるメッセージを生成してサビスデータ—ジ情報処理手段へ送信し、サビスデータ—ジ情報処理手段が、このメッセージを受信し、支払手段との通信回路の接続を知らせるメッセージを生成して、請求手段へ送信するようにしたものであり、商売における秘密漏洩や成りすましてなる不正決済の発生を防止し、効率的に関与合致コールの処理を行なうことが、できる。

【0055】請求項76に記載の発明は、決済手段の第2の決済手段と連携しているデータの変更を要求するメッセージングを生成して支払手段または請求手段に送信した場合に、支払手段または請求手段の中央処理装置が、第2の決済手段と連携しているデータを含むメッセージングを生成して決済手段またはサード提供手段に送信し、これを受けた決済手段またはサード提供手段が、支払手段または請求手段の第2の決済手段の更新データを含むメッセージングを生成して支払手段または請求手段に送信し、支払手段または請求手段の中央処理装置がメッセージングから更新データを手取り出し

(23)

て第2の蓄積手段に蓄積されているデータを更新するよううにしたいものであり、サービス提供手段が、支払手段の第2の蓄積手段、または、請求手段の第2の蓄積手段に蓄積されている情報と、強制的に更新することができ、契約内容が変わった場合など、支払手段の第2の蓄積手段、または、請求手段の第2の蓄積手段に蓄積されている情報を更新する必要がある場合に有効である。

【0096】請求項77に記載の発明は、決済手段を、分散して配置された複数の決済手段によって構成し、それらの決済手段を通信網で相互に接続したものであり、決済手段の処理を分散させて行なうことにより、処理効率が向上する。

【0097】請求項78に記載の発明は、増数の決着手段を、地域ごとに、または、組織ごとに分散して配置しており、決着手段の処理を、地域または組織ごとに分散させることにより、処理の効率が向上する。

〔10098〕請求項79に記載の説明は、支払手段及び支払手段の所有者に関する情報が、支払手段または支払手段の所有者と同じ属性を有する決済手段の第1の蓄積手段に蓄積され、請求手段または請求手段の所有者に関する情報が、請求手段または請求手段の所有者に属する情報を有する決済手段の第2の蓄積手段に蓄積され、全ての決済手段の第1の蓄積手段には、さらに、その決済手段と通信が許される全ての支払手段の識別情報と、支払手段及び支払手段の所有者に関する情報が蓄積されている場所を示す位置情報とが蓄積され、全ての決済手段の第2の蓄積手段には、さらに、その決済手段及び通信が許される全ての請求手段の識別情報と、請求手段及び通信が許される請求手段に関する情報とが蓄積されている場所を示す位置情報とが蓄積されるようにしたものであり、各決済手段で、支払手段に関連する情報及び支払手段の所有者に関連する情報と、請求手段に関連する情報及びその所有者に関連する情報とを効率的に蓄積管理する手段と通信をしても、それらの情報にアクセスできる。請求手段が、支払手段または請求手段は、どの決済手段と通信をしても、それらの情報にアクセスできる。

【10099】請求項80に記載の発明は、サービス提供手段を、分散して配置された複数のサービス提供手段によって構成し、それらのサービス提供手段を通信回線によって相互に接続したものであり、サービス提供手段の処理を分散させて行なうことにより、処理の効率が向上する。

【0100】請求項81に記載の発明は、複数のサービス提供手段を、地域ごとに、または、組織ごとに分散して配置したものであり、サービス提供手段の処理を、地域または組織ごとに分散させることにより、処理効率が向上する。

(0101) 請求項8に記載の発明は、支払手段及び支払手段の所有者に関する情報が、支払手段または支払手段の所有者と同じ属性を有するサービス提供手段の所有主の登録手段に蓄積され、請求手段及び請求手段の所有者の登録手段に蓄積される。

者に、請求手段または請求手段の所有者と同一属性を有するサービス提供手段の第2の蓄積手段に蓄積され、全てのサービス提供手段の第1の蓄積手段に蓄積され、さらに、そのサービス提供手段との属性が許されるのは、全てのサービス提供手段と、支払手段及び支払手段の所有者に関する情報が蓄積されている場所を示す位置情報とが蓄積され、全てのサービス提供手段の第2の蓄積手段には、さらに、そのサービス提供手段との属性が許される全ての請求手段の識別情報と、請求手段及び請求手段の所有者に関する情報が蓄積されている場所を示す位置情報とが蓄積されるようにしたものであり、各サービス提供手段で、支払手段に関連する情報及び支払手段の所有者に関連する情報と、請求手段に関連する情報及びサービス提供手段の所有者に関連する情報とを効率的に蓄積管理することができ、支払手段または請求手段は、どのサービス提供手段と属性をしても、それらの情報にアクセスすることができ、

【0102】請求項83に記載の説明は、この図性が、「組織」であるようにしたものであり、請求手段やその所有者、あるいは、支払手段やその所有者に関する情報が、その所有者が属する組織の決済手段やサービス提供手段に蓄積管理される。

【0103】請求項84に記載の説明は、この図性が、「地域」であるようにしたものであり、請求手段とその所有者、あるいは、支払手段やその所有者に関する情報が、その所有者が在住する地域の決済手段やサービス提供手段に蓄積管理される。

【0104】請求項8に記載の発明は、支払手段が、第2のサービス提供手段と通信回線を接続し、この第2のサービス提供手段が、支払手段及び支払手段の所有者のサービス提供手段に関する情報を第1のサービス提供手段と相連する場合に、第2のサービス提供手段のサービスマネージャ情報処理手段が、第2のサービス提供手段の第1の業務手段に蓄積されている支払手段の識別情報と、支払手段及び支払手段の所有者に関する情報が蓄積されている場所を示す位置情報とから、第1のサービス提供手段を特定し、第1のサービス提供手段のサービスマネージャ情報処理手段に支払手段に対応するホームユーザ情報処理手段の生成を要求し、ホームユーザ情報処理手段が、第1のサービス提供手段上生成された場合に、支払手段に対応するモバイルユーザ情報処理手段を第2のサービス提供手段上生成し、生成されたモバイルユーザ情報処理手段とホームユーザ情報処理手段とが、連携して、支払手段との通信と、支払手段及び支払手段の所有者に関する情報の処理とを行なうようにしたものであり、支払手段はどのサービス提供手段と通信回線を接続しても、その支払手段及び支払手段の所有者に関する情報にアクセスすることができ、効率的に決済処理を行うことができる。

【0105】請求項86に記載の発明は、支払手段が、

第2のサービス提供手段のユーザが情報処理手段と通信手段を接続して、支払処理の取消処理を要求し、この第2のサービス提供手段が、支払処理に因関した請求手段及びその所有者に関する情報を蓄積する第1のサービス提供手段と相違する場合には、第2のサービス提供手段のサービスマネージャ情報処理手段が、第2のサービス提供手段のサービスの第2の蓄積手段に蓄積されている請求手段の識別情報が、第1のサービス提供手段の所有者に関する情報に異なる情報があることを示す位置情報とから、第1のサービス提供手段を特定し、第1のサービス提供手段のサービスマネージャ情報処理手段に、ユーザ情報処理手段から受領した支払処理の取消を要求するメッセージを送信し、第1のサービス提供手段のサービスマネージャ情報処理手段が、第1のサービス提供手段のマーチャント情報処理手段から受領した決済処理の取消処理を要求するメッセージと、第2のサービス提供手段のサービスマネージャと、第2のサービス提供手段のユーザ情報処理手段とを照合して、第1のサービス提供手段のサービスマネージャ情報処理手段から受領した決済処理の取消処理を要求するメッセージと、第2のサービス提供手段のユーザ情報処理手段のグループを定義するようにしたことから成る情報処理手段の動作とを特徴とする。

【0106】請求項8に「既知の列明は、請求手段が、第2のサービス提供手段のマーケティング情報処理手段に「支払手段との通信を要求するメッセージング」を送信し、この第2のサービス提供手段が、支払手段及びその所有者に関する情報を蓄積する第1のサービス提供手段と相連する場合には、マーケティング情報処理手段から「支払手段との通信を要求するメッセージ」を受信した第2のサービス提供手段のサービスマネージャ情報処理手段が、第2のサービス提供手段上にサービスディレクタ情報処理手段を生成して、マーケティング情報処理手段とサービスディレクタ情報処理手段とから成る情報処理手段のグループを定義し、生成されたサービスディレクタ情報処理手段が、要求先の支払手段とその所有者とを特定し、特定した支払手段に対応するユーザ情報処理手段をグループへ追加するようにサービスマネージャ情報処理手段に要求し、それを受けてサービスマネージャ情報処理手段が、第2のサービス提供手段の第1の蓄積手段に蓄積されている支払手段の識別情報と、支払手段及び支払手段の所有者に関する情報が蓄積されている場所を示す位置情報とから、第1のサービス提供手段を特定し、第1のサービス提供手段のサービスマネージャ情報処理手段に支払手段に対応するユーザ情報処理手段の生

成を要求し、第1のサービス提供手段上に、支払手段に  
対応するユーザ情報処理手段が生成された場合に、その  
ユーザ情報処理手段をグループに追加するようにしたも  
のであり、請求手段は、他のサービス提供手段が管理す  
る支払手段とも連係を行なうことができる。

【0107】請求項8に記載の発明は、支払手段が、第2のサービス提供手段のユーザが情報処理手段に「請求手段との通信を要求するメッセージ」を送信し、この第2のサービス提供手段が、請求手段及びその所有者に関する情報を蓄積する第1のサービス提供手段と相違する場合に、ユーザが情報処理手段から「請求手段との通信を要求するメッセージ」を受信した第2のサービス提供手段のサービスマネージャ情報処理手段が、第2のサービス提供手段の第2の蓄積手段に蓄積されている請求手段の識別情報と、請求手段及び請求手段の所有者に関する情報を蓄積されている場所を示す位置情報とから、第1のサービス提供手段を特定し、第1のサービス提供手段のサービスマネージャ情報処理手段に、ユーザが情報処理手段から受信した「請求手段との通信を要求するメッセージ」を送信し、このメッセージを受信した第1のサービス提供手段のサービスマネージャ情報処理手段が、第1のサービス提供手段上にサービスディレクトリタ情報処理手段を生成して、このサービスディレクトリ情報処理手段と第2のサービス提供手段上のユーザ情報処理手段とからなる情報処理手段のグループを定義し、生成されたサービスディレクトリ情報処理手段が、要求先の請求手段に対応するマーチャント情報処理手段をグループへ追加するように第1のサービス提供手段のサービスマネージャ情報処理手段に要求し、それを受けて、サービスマネージャ情報処理手段が、第1のサービス提供手段上に、請求手段に対応するマーチャント情報処理手段を生成して、グループに追加するようにしたものであり、支払手段は、どのサービス提供手段と通信回線を接続し、どの支払手段に属連する情報及び支払手段の所有者に関する情報を蓄積しているサービス提供手段と通信回線を接続した場合と同様に、請求手段との通信を行なうことができる。

【0108】請求項89に記載の発明は、支払手段に、蓄積手段として、強弱電体メモリを設けたものであり、支払手段のバッテリーの寿命が伸びる効果がある。

【0109】請求項90に記録の発明は、請求項5乃至89に記録の支払手段の中央処理装置の制御プログラムラムを、電子計算機が読み取り可能な形式で記録媒体に記録したものであり、プログラムを、持ち運び可能な形態で提供されることができる。

【0110】請求項9に記載の発明は、請求項6乃至89に記載の請求手段の中央処理装置の制御プログラムを、電子計算機が読み取り可能な形式で記録媒体に記録したものであり、プログラムを、持ち運び可能な形態で提供することができる。



を受発信するアンテナ。2011は、レシーバ・スビーカ。3013は、120×160画素表示のカラー液晶ディスプレイ（LCD）。2041は、パーソナル・クレジット端末100の動作モードを切り替えるモードスイッチ。2051は、デジタル無線電話の通話スイッチ。2012は、デジタル無線電話の終了スイッチ。2011は、フアンクションスイッチ。208は、テンキースイッチ。2013は、電源スイッチ。2101は、マイクである。

【0134】さらに、図2（b）において、211は、代金の支払や、決済内容の確認、クレジッド取引の取消など、ユーザの操作をともなう処理の実行を促す実行スイッチ。212は、ヘッドセットを接続するためのヘッドセット用ジャックである。

【0135】パーソナル・クレジット端末100には、クレジットカードモードとデジタル無線電話モードとの2つの動作モードがあり、モードスイッチ204によって切り替わる。パーソナル・クレジット端末100は、デジタル無線電話モードでは、デジタル無線電話として動作し、クレジットカードモードでは、電子的なクレジット決済手段、つまり、電子的なクレジットカードとして動作する。

【0136】電子的なクレジットカードは、ユーザによるクレジットカード会社とのクレジットサービスとの会員契約を前提として、パーソナル・クレジット端末100に登録される。ユーザが、複数のクレジットサービスとの会員契約をしている場合には、複数のクレジットカードが、端末100に登録される。

【0137】このパーソナル・クレジット端末100を用いて、例えば電話をかける場合には、ユーザは、まず、モードスイッチ204で、動作モードをデジタル無線電話モードにし、次に、テンキースイッチ208で電話番号を入力して、通話スイッチ206を押す。以上の操作で、ユーザは、入力した電話番号に電話をかけることが出来る。

【0138】また、パーソナル・クレジット端末100に電話が来て来た場合には、パーソナル・クレジット端末100は、その時の動作モードに関係なく、発信音を発する。この場合には、通話スイッチ206を押すことで自動的にデジタル無線電話モードに切り替わり、ユーザは電話を受けることが出来る。

【0139】また、アンテナにクレジットで代金を支払う場合には、まず、モードスイッチ204により動作モードをクレジットカードモードに設定し、フアンクションスイッチ207で、支払に使用するクレジットカードを選択する。次に、テンキースイッチ208で、支払金額を入力し、赤外線通信ポート20をアンテナのクレジット決済装置101の方向に向けて、実行スイッチ211を押す。以上の操作によって、パーソナル・クレジット端末100は、クレジット決済装置101と間で赤外線通信を行ない、それとともにサービス提供システム103との

【0111】請求項92に記載の説明は、請求項7乃至89に記載の決済手段の計算機システムの処理プログラムを、電子計算機が読み取り可能な形式で記録媒体に記録したものであり、プログラムを、持ち運び可能な形態で配送させることができる。

【0112】請求項93に記載の説明は、請求項40乃至89に記載のサービス提供手段の計算機システムの処理プログラムを、電子計算機が読み取り可能な形式で記録媒体に記録したものであり、プログラムを、持ち運び可能な形態で配送させることができる。

【0113】請求項94に記載の説明は、請求項40乃至89に記載の決済処理手段の計算機システムの処理プログラムを、電子計算機が読み取り可能な形式で記録媒体に記録したものであり、プログラムを、持ち運び可能な形態で配送させることができる。

【0114】以下、本発明の実施の形態について、図面を用いて説明する。

【0115】（実施の形態1）本発明の第1の実施形態について、図1から図41を用いて説明する。

【0116】第1の実施形態のクレジット決済システムは、個人消費者が、一般の小売販売店で購入する際に、消費者が小売販売店との間で、クレジットカードや利用明細などを直接受け渡すことなく、無線通信によって、クレジット決済を行なうシステムであり、これをパーソナル・リモート・クレジット決済システムと呼び、このシステムによって提供されるクレジット決済サービスを、パーソナル・リモート・クレジット決済サービスと呼ぶこととする。

【0117】このパーソナル・リモート・クレジット決済システムは、図1のシステム構成図に示すように、2系統の双方向無線通信機能と電子的なクレジットカード機能とを持つパーソナル・クレジット端末100と、小売販売店におけるクレジット決済処理を行なうクレジット決済装置101と、クレジットサービス会社または決済処理会社におけるクレジット決済処理を行なう決済システム103と、パーソナル・クレジット端末100、クレジット決済装置101及び決済システム103を結ぶ通信ネットワークの中心に位置してパーソナル・リモート・クレジット決済サービスを提供するサービス提供システム102と、ネットワークにおけるデータ伝送路を提供するデジタル公衆網106と、パーソナル・クレジット端末100をデジタル公衆網106に接続する無線電話の基地局104とを備えている。

【0118】パーソナル・クレジット端末100は、赤外線とデジタル無線電話との2系統の双方向無線通信機能と、電子的なクレジットカードの機能とを持つ携帯無線電話端末である。また、小売販売店におけるクレジット決済処理を行なうクレジット決済装置101も、赤外線通信とデジタル電話通信との2系統の双方向通信機能を持つ。

【0119】なお、図1において、1051は、パーソナル・クレジット端末100とクレジット決済装置101との間で行なう赤外線通信の伝送路、1061は、パーソナル・クレジット端末100と基地局104との間で行なうデジタル公衆網の伝送路を示し、1071は、基地局104とデジタル公衆網106とを結ぶデジタル通信回線、1091は、デジタル公衆網106とサービス提供システム103とを結ぶデジタル通信回線、1101は、クレジット決済装置101とデジタル公衆網106とを結ぶデジタル電話通信回線、1111は、サービス提供システム103と決済システム103とを結ぶデジタル通信回線を示している。

【0120】パーソナル・リモート・クレジット決済サービスは、通常の運用形態としては、次のような形態を想定している。

【0121】決済システム103は、クレジットカード会社または決済処理会社は、クレジット決済装置101は、小売販売店に設置され、パーソナル・クレジット端末100を、消費者が持ち歩く、サービス提供システム102は、パーソナル・リモート・クレジット決済サービスを提供する会社は設置され、クレジットカード会社がパーソナル・リモート・クレジット決済サービスを、サービス提供システム103は、クレジットカード会社に設置される。

【0122】また、前提として、消費者は、クレジットカード会社との間で、クレジットサービスとの会員契約を、パーソナル・リモート・クレジット決済サービスを提供する会社との間では、パーソナル・クレジット決済サービスとの会員契約を、さらに、電話会社との間では、無線電話サービスとの契約を結んでいる。同様に、小売販売店も、クレジットカード会社との間で、クレジットサービスとの加盟店契約を、パーソナル・リモート・クレジット決済サービスを提供する会社との間で、パーソナル・リモート・クレジット決済サービスとの加盟店契約を、さらに、電話会社との間で、デジタル電話通信サービスとの契約を結んでいる。

【0123】また、パーソナル・リモート・クレジット決済サービスが、クレジットカード会社とは別会社によって提供される場合には、パーソナル・リモート・クレジット決済サービスを提供する会社は、クレジットカード会社との間で、クレジットサービスに契約している会員に対して、クレジットカード会社の代わに、電子的なクレジットカードを発行し、パーソナル・リモート・クレジット決済サービスを運営する契約を結んでいる。

【0124】また、決済処理会社が、決済システム103を用いてクレジット決済処理を行なう場合には、クレジットカード会社は、決済処理会社との間で、クレジット決済処理を、決済処理会社が代行する契約を結んでいる。

【0125】以下では、本システムの説明を簡便にするために、パーソナル・クレジット端末100の所有する消費者をユーザ（user）、クレジット決済装置101を設置し

た小売販売店をマーチャント（Merchant）、クレジット決済装置101を操作する販売店員を担当者（operation）、パーソナル・リモート・クレジット決済サービスを、提供する会社をサービス提供者（Service Provider）、決済システム103を用いてクレジット決済処理を行なうクレジットカード会社または決済処理会社を決済処理機関（Transaction Processor）と呼ぶこととする。

【0126】本システムでは、ユーザがマーチャントに対して商品の代金をクレジットによって支払う場合、パーソナル・クレジット端末100、クレジット決済装置101及びサービス提供システム103の三者間で電子的に決済情報を交換し、さらに、サービス提供システム102と決済システム103との間で電子的に決済情報を交換することによって、クレジット決済処理を行なう。

【0127】基本的には、サービス提供システム102が、パーソナル・クレジット端末100とクレジット決済装置101とを、それぞれ、支払要求と決済要求とを受け取り、支払要求と決済要求とを照合し、ユーザとマシントとに代わって、決済システム103に決済処理を要求する。そして、決済システムが順順の決済処理を行なう。

【0128】この時、パーソナル・クレジット端末100とクレジット決済装置101とは、伝送路105を用いて、赤外線通信を行ない、パーソナル・クレジット端末100とサービス提供システム103とは、伝送路106及び基地局104、さらに、デジタル公衆網106及びデジタル公衆網108及びデジタル通信回線109を介して、デジタル無線電話を行ない、デジタル無線電話によるデジタル電話通信を行ない、クレジット決済装置101とサービス提供システム102とは、デジタル電話通信109を介してデジタル電話通信を行なう。そして、サービス提供システム102と決済システム103とは、デジタル通信回線111を介して、デジタルデータ通信を行なう。

【0129】パーソナル・クレジット端末100とサービス提供システム102との通信、クレジット決済装置101とサービス提供システム102との通信、及び、サービス提供システム102と決済システム103との通信では、交換される決済情報も、全て、暗号化して通信する。暗号化には、秘密鍵方式の暗号処理と公開鍵方式の暗号処理とを組み合わせて、情報を電子封鎖化して通信する。

【0130】次に、本システムを構成する各構成要素について説明する。

【0131】まず、パーソナル・クレジット端末100について説明する。

【0132】図2（a）、図2（b）は、それぞれ、パーソナル・クレジット端末100の前面側及び背面側の外観図である。

【0133】図2（a）において、2001は、クレジット決済装置101と赤外線通信を行なう赤外線通信ポート（赤外線受光部）。

2011は、デジタル無線電話の電波

(27)

間でデジタル無線電話通話を行ない、それぞれ、決済情報と交換して、クレジット決済処理を行なう。パーソナル・クレジット端末100の内部の構成と詳細な動作とについては、後で説明する。

【0140】次に、クレジット決済装置101について説明する。

【0141】図3は、クレジット決済装置101の外観図である。この装置は、クレジット決済処理の機能とデジタル電話の機能とを持つクレジット決済端末300と、商品の代金を計算するキャッシュレジスタ311と、クレジット決済端末300及びキャッシュレジスタ301を接続するRS-232Cケーブル313と、シリアルケーブル310を介してクレジット決済端末300に接続する赤外線受発光モジュール301とを備えている。

【0142】図3において、302は、3.20×2.40画素表示のカラード液晶ディスプレイ(LCD)、303は、受話器、304は、クレジット決済端末300の動作モードを切り替えるモードスイッチ、305は、電話のフックスイッチ、306は、ファンクションスイッチ、307は、テンキー、308は、代金の支払、決済内容の確認、クレジット取引の取消など、マーチャントの機能をともなう処理の実行を促す実行スイッチ、309は、電源スイッチであり、また、312は、キャッシュレジスタ311のクレジットによる決済処理を指定するクレジット決済スイッチである。

【0143】クレジット決済端末300には、クレジット決済モードとデジタル電話モードとの2つの動作モードがあり、モードスイッチ304によって切替る。デジタル電話モードでは、デジタル電話機として動作し、クレジット決済モードでは、パーソナル・リモート・クレジット決済サービスのクレジット決済処理端末として動作する。

【0144】このクレジット決済端末300から、例えば電話をかける場合には、担当者は、まず、モードスイッチ304で、動作モードをデジタル電話モードにし、次に、テンキー307で電話番号を入力する。以上

の操作によって、担当者は、入力した電話番号に電話をかけることが出来る。

【0145】また、クレジット決済端末300に電話がかかって来た場合には、クレジット決済端末300は、動作モードに關係なく、着信音を流す。この場合には、電源303を上げるか、フックスイッチ305を押すことで、自動的に電話モードに切り替わり、担当者は電話を受けることが出来る。

【0146】また、クレジット決済処理を行なう場合には、まず、キャッシュレジスタ311で、商品価格と税金等から合計金額を計算し、その金額をユーザに伝える。次に、クレジットによる支払を希望するユーザの要望にしたがって、キャッシュレジスタ311のクレジット決済スイッチ312を押し、ユーザがパーソナル・クレジット

端末100で代金の支払操作を行なうのを待つ。ユーザが、代金の支払操作を行なうと、ユーザが入力した支払金額がLCD302に表示され、さらに、ユーザの信用照会の結果が表示される。担当者はその内容を確認して、実行スイッチ308を押す。

【0147】以上の操作によって、クレジット決済装置101は、パーソナル・クレジット端末100、及びサービス提供システム102と、それぞれ、決済情報を交換して、クレジット決済処理を行なう。クレジット決済端末300の内部の構成と詳細な動作については、後で説明する。

【0148】次に、サービス提供システム102について説明する。

【0149】図4は、サービス提供システム102のプロック構成図である。サービス提供システム102は、パーソナル・リモート・クレジット決済サービスにおいて、パーソナル・クレジット端末100、クレジット決済装置101、及び決済システム103のそれぞれと交換する決済情報のデータ処理とその際のデータ通信の制御とを行なうサービスサーバ400と、ユーザ、マーチャント、及び決済処理装置に関する属性情報とサービス提供システム102が提供するサービスの属性情報とを管理するサービスディレクタ情報サーバ401と、ユーザの属性情報とパーソナル・クレジット端末100内のデータとを管理するユーザ情報サーバ402と、マーチャントの属性情報とクレジット決済端末300内のデータとを管理するマーチャント情報サーバ403と、決済処理装置の属性情報と決済処理の属性情報とを管理する決済処理装置情報サーバ404と、サービス提供者がサービス提供システム102の運用と、サービス提供システム407とを備えており、各サーバ400～404及び管理システム407は1台または複数のコンピュータで構成されている。

【0150】また、サービスサーバ400、サービスディレクタ情報サーバ401、ユーザ情報サーバ402、マーチャント情報サーバ403及び決済処理装置情報サーバ404は、それぞれ、ATM-LANケーブル408、410、411、412、413によってATM-LANスイッチ405に接続され、サービスサーバ400は、ATM-LANスイッチ405を介して、サービスディレクタ情報サーバ401、ユーザ情報サーバ402、マーチャント情報サーバ403、または決済処理装置情報サーバ404にアクセスする。

【0151】また、ATM-LANスイッチ405は、ATM-LANケーブル415によって、ATM交換機506に接続される。ATM交換機506には、デジタル公衆網108と結ぶデジタル通信回線109と、決済システム103と結ぶデジタル通信回線111とが接続され、サービスサーバ400は、ATM-LANスイッチ405及びATM交換機506を介して、パーソナル・クレジット端末100、クレジット決済装置101、及び決済システム103と通信を行なう。

【0152】管理システム407は、ATM-LANケーブル414によって、ATM-LANスイッチ405に接続さ

(28)

れ、さらに、ATM-LANケーブル416によって、ATM交換機406に接続される。管理システム407は、ATM-LANスイッチ408、ATM交換機406、及びATM-LANスイッチ405を介して、サービスサーバ400、サービスディレクタ情報サーバ401、ユーザ情報サーバ402、マーチャント情報サーバ403、または決済処理装置情報サーバ404にアクセスして、サービス提供システム102の運用管理を行なう。

【0153】ATM交換機406は、サービス提供システム102の外部と内部との通信、及びサービス提供システム102の内部間の通信において、データ通信の交換機として動作する。また、ATM交換機406は、複数の通信方式に対応し、通信アダプタの機能を持つ。例えば、サービスサーバ400とクレジット決済装置101との通信では、まず、クレジット決済装置101とATM交換機406との間で、ISDNのデータパケットを交換し、ATM交換機406が、ISDNのデータパケットからATMパケットへの変換、及び、その逆変換を行ない、ATM交換機406とサービスサーバ400との間で、ATMパケットを交換する。同様に、サービスサーバ400とパーソナル・クレジット端末100との間の通信、サービスサーバ400と決済システム103との間の通信においても、ATM交換機406が、それぞれの通信方式に対応して、通信データの変換を行なう。

【0154】また、パーソナル・クレジット端末100-サービス提供システム102間、及び、クレジット決済装置101-サービス提供システム102間の通信費用を軽減するために、通常、サービス提供システム102は、パーソナル・リモート・クレジット決済サービスを提供する地域ごとに設置される。したがって、ATM交換機406には、他の地域のサービス提供システムと結ぶ専用デジタル通信回線417が接続される。この場合、サービス提供システム102同士は、お互いにデータと共有し、協調してデータ処理を行なう。

【0155】次に、決済システム103について、簡単に説明する。

【0156】図5は、決済システム103のプロック構成図である。決済システム103は、パーソナル・リモート・クレジット決済サービスにおいて、サービス提供システム102と交換する決済情報のデータ処理を行なうトラディショナル処理サーバ500と、クレジットサービスの加入者の個人情報と管理する加入者情報サーバ501と、クレジットサービスの加盟店の情報を管理する加盟店情報サーバ502と、クレジット決済の取引情報を管理する取引情報サーバ503と、決済処理装置が決済システム103の運用管理を行なう管理システム506とを備えており、各サーバ500～503、及び管理システム506は、一台、あるいは、複数のコンピュータによって構成される。

【0157】また、トラディショナル処理サーバ500、加入者情報サーバ501、加盟店情報サーバ502、及び取引

情報サーバ503は、それぞれ、ATM-LANケーブル508、8.609.610.611によって、ATM-LANスイッチ504に接続され、トラディショナル処理サーバは、ATM-LANスイッチ504を介して、加入者情報サーバ501、加盟店情報サーバ502、または取引情報サーバ503にアクセスする。

【0158】また、ATM-LANスイッチ504は、ATM-LANケーブル513によって、ATM交換機505に接続される。ATM交換機505には、サービス提供システム102と結ぶデジタル通信回線111が接続され、トラディショナル処理サーバは、ATM-LANスイッチ504及びATM交換機505を介して、サービス提供システム102と通信を行なう。

【0159】パーソナル・リモート・クレジット決済サービスにおいて、決済システム103が行なうクレジット決済処理は、サービス提供システム102からの決済要求に対して、トラディショナル処理サーバ500が、加入者情報サーバ501、加盟店情報サーバ502、及び取引情報サーバ503の情報を、それぞれ更新することによって成立する。

【0160】また、ATM交換機505には、サービス提供システム102と結ぶデジタル通信回線111の他に、銀行オンラインシステムと結ぶ銀行専用回線516、さらに、他の決済処理装置の決済システムと結ぶ専用デジタル通信システム、及び、他の決済処理装置の決済システムと通信を行ない、金融機関間の決済処理を行なう。

【0161】管理システム506は、ATM-LANケーブル512によって、ATM-LANスイッチ504に接続され、さらに、ATM-LANケーブル514によって、ATM交換機505に接続される。管理システム506は、ATM-LANスイッチ507、ATM交換機505、及びATM-LANスイッチ504を介して、トラディショナル処理サーバ500、加入者情報サーバ501、加盟店情報サーバ502、または取引情報サーバ503にアクセスし、決済システム103の運用管理を行なう。

【0162】ATM交換機505は、決済システム103の外部と内部との通信、及び決済システム103の内部間の通信において、データ通信の交換機として動作する。また、ATM交換機505は、複数の通信方式に対応した、通信アダプタの機能を持ち、トラディショナル処理サーバ500とサービス提供システム102との間の通信、トラディショナル処理サーバ500と銀行オンラインシステムととの間の通信、トラディショナル処理サーバ500と他の決済処理装置の決済システムとの間の通信において、ATM交換機506が、それぞれの通信方式に対応して、通信データの変換を行なう。

【0163】次に、本システムが提供するパーソナル・リモート・クレジット決済サービスについて説明する。

【0164】パーソナル・リモート・クレジット決済サ

(139)

ービスには、大きく分けて、“決済”、“キャンセル”、“顧客サービスコール”、及び、問い合わせコール”の4つ処理がある。

【0165】“決済”は、ユーザがユーザインタフェースで支払うクレジット決済を、クレジットカードや利用明細書などを、直接受け置きことなく、無償通信によって行なう処理。“キャンセル”は、パーソナル・リモート・クレジット決済サービスの“決済”の処理によって完了した取引を、ユーザとユーザインタフェースとの合意の基に、無償通信によって、取り消す処理。“顧客サービスコール”は、パーソナル・リモート・クレジット決済サービスの“決済”の処理によって取引のあったユーザに対して、ユーザインタフェースの電話番号を知らない場合でも、電話連絡を可能にする処理。そして、“問い合わせコール”は、パーソナル・リモート・クレジット決済サービスの“決済”の処理によって取引のあったユーザインタフェースに対して、ユーザが自分の電話番号を知られることなく、問い合わせの電話を可能にする処理である。

【0166】まず、“決済”の処理の流れを説明する。  
【0167】図6Aは、パーソナル・リモート・クレジット決済サービスの“決済”の処理の流れを示している。また、図7の(a)～(h)は、上記の“決済”の処理に例示する、図8の(a)～(h)は、クレジット決済増減300のLCD302の表示例を示している。

【0168】図7 (a)は、パーソナル・クレジット端末がデジタル無線電話モードの時の初期画面であり、図7 (b)は、クレジットカードモードの時の初期画面、図8 (a)は、クレジット決済増減300のクレジット決済モードの時の初期画面であり、図8 (b)は、クレジット決済モードの時の初期画面である。

【0169】“決済”の処理は、まず、ユーザが担当者に購入するものを提示して、担当者がその商品の金額を計算するところから始まる。

【0170】図6では、まず、担当者が、クレジット決済装置のキヤッシュレジスタ311を用いて、代金の合計金額を計算する(キヤッシュレジスタで、請求金額を計算600)。すると、キヤッシュレジスタは、計算した合計金額を表示する(請求金額の表示601)。担当者は、ユーザに、商品の代金の合計金額を伝え、支払方法を尋ねる(請求金額を提示し、支払方法を尋ねる602)。ユーザは、パーソナル・リモート・クレジット決済サービスの“決済”を希望し(パーソナル・リモート・クレジット決済サービスの“決済”を指示603)、それに対して担当者は、クレジット決済装置のクレジット決済スイッチ313を押して(クレジット決済スイッチを押す604)、ユーザに、パーソナル・クレジット増減1000の支払操作を始めるように指示する(支払操作の開始を指示605)。この時、キヤッシュレジスタ311が、RS-23

2Cケーブル313を介して、クレジット決済増減300に、クレジット決済命令が送信される。クレジット決済増減300は、自動的にクレジット決済モードになり、LCD302には図8 (c) のような画面を表示する(支払操作待ち表示606)。

【0171】ユーザは、パーソナル・クレジット増減1000を、モードスイッチ204でクレジットカードモードに、フアンクションスイッチ207で、LCD303に表示されるクレジットカードを切り替え、支払に使用済クレジットカードを選択する。この時、パーソナル・クレジット増減1000は、図7 (b) の画面から図7 (c) の画面になる。さらに、フアンクションスイッチ207で、メニューの中から“支払”を選択し、実行スイッチ311を押す。すると、パーソナル・クレジット増減1000は、図7 (d) の画面になる。ユーザは、図7 (e) のように、テンキースイッチ208で支払う金額を入力し、フアンクションスイッチ307で支払オプションを指定して、実行スイッチ311を押す。すると、図7 (f) の確認画面が表示され、ユーザは、赤外線通信ポート300をクレジット決済増減300に向けて実行スイッチ311を押す(支払操作607)。すると、パーソナル・クレジット増減100は、支払金額を示すメッセージ、支払オプション=608を、赤外線通信によってクレジット決済装置10へ送信する。

【0172】クレジット決済増減300は、支払オプション=608を、赤外線受光モジュール301から受信し、その中の支払金額と請求金額とを照合して、支払オプションに対する応答メッセージ、支払オプション=609を、赤外線通信によってパーソナル・クレジット増減300へ送信する。さらに、クレジット決済増減300は、ユーザの信用照会を要求するメッセージ、信用照会要求610を、デジタル無線通信で、サービス提供システム102へ送信する。この時、クレジット決済増減300は、図8 (d) の画面になる(信用照会中表示611)。

【0173】一方、パーソナル・クレジット増減100は、赤外線通信ポート200から支払オプション=609を受信し、その中の請求金額と支払金額とを照合して、クレジットによる代金の支払を要求するメッセージ、支払要求613を、デジタル無線通信で、サービス提供システム102に送信する。この時、パーソナル・クレジット増減100は、図7 (g) の画面を表示する(支払処理実行中表示612)。

【0174】サービス提供システム102は、クレジット決済増減300からの信用照会要求610と、パーソナル・クレジット増減100からの支払要求613とをそれぞれ受信し、それらの内容を照合し、さらに、ユーザの信用状況を調べ、信用照会要求に対する応答メッセージ、信用照会応答614を生成して、クレジット決済増減300へ送信する。

【0175】クレジット決済増減300は、サービス提供

(140)

システム102からの信用照会応答614を受信し、図8 (e) のように、信用照会応答614の内容を表示して、信用照会の結果を担当者に知らせる(信用照会結果表示615)。

【0176】担当者は、信用照会結果を確認し、クレジット決済増減300の実行ボタン308を押して、決済処理の開始を指示する(決済処理要求操作616)。すると、クレジット決済増減300は、決済処理を要求するメッセージ、決済要求617を、デジタル無線通信で、サービス提供システム102へ送信し、図8 (f) の画面を表示する(決済実行中表示618)。

【0177】サービス提供システム102は、クレジット決済増減300からの決済要求617を受信し、決済システム103に対して決済処理を要求するメッセージ、決済要求619を、決済システム103へ送信する。A 決済システム103は、サービス提供システム102からの決済要求619を受信し、決済処理を行ない、決済処理が完了したことを示すメッセージ、決済完了通知620を、サービス提供システム102へ送信する。

【0178】サービス提供システム102は、決済システム103からの決済完了通知620を受信し、クレジット決済増減300に対して、決済処理が完了したことを示すメッセージ、決済完了通知621を送信する。

【0179】クレジット決済増減300は、決済完了通知621を受信し、図8 (g) のように、決済完了通知621の内容を表示して、決済処理が完了したことを、担当者に知らせる(決済完了表示622)。さらに、クレジット決済増減300は、電子的な領収書623を発行し、デジタル電話通信で、サービス提供システム102へ送信する。

【0180】サービス提供システム102は、クレジット決済増減300が発行した領収書623を受信し、パーソナル・クレジット増減100用のデータ・フォーマットに変換した領収書624を生成し、デジタル無線通信で、パーソナル・クレジット増減100へ送信する。

【0181】パーソナル・クレジット増減100は、サービス提供システム102からの領収書624を受信し、図7 (h) のように、領収書624の内容を表示して、決済処理が完了したことを、ユーザに知らせる(領収書表示625)。

【0182】以上のようにして、パーソナル・リモート・クレジット決済サービスの“決済”の処理は行なわれる。上記の“決済”の処理において、機器間で交換されるデータの内部の詳細については、後で説明する。

【0183】次に、“キャンセル”の処理の流れを説明する。  
【0184】図9は、パーソナル・リモート・クレジット決済サービスの“キャンセル”の処理の流れを示している。

【0185】また、図10の(a)～(h)は、上記の“キャンセル”の処理において、パーソナル・クレジット

増減1000のLCD302の表示例を示し、図11の(a)～(h)は、クレジット決済増減300のLCD302の表示例を示している。

【0186】パーソナル・リモート・クレジット決済サービスの“キャンセル”の処理を行なう状況としては、ユーザとユーザインタフェースが、お互い内容が読めるほどの近距離にいる場合と、遠距離に離れている場合とがある。二つの場合の違いは、最初の“キャンセル”の処理に関するユーザとユーザインタフェースとの合意を、音声による話し合いで行なうか、電話によって行なうかの違いであり、両者の合意の後の処理の流れは同じである。したがって、ここでは、両者が遠距離に離れている場合について説明する。

【0187】“キャンセル”の処理は、まず、一度、“決済”の処理によって完了した取引に対して、“キャンセル”の処理を行なうことを、ユーザとユーザインタフェースの担当者とが合意するところから始まる。

【0188】図9では、まず、ユーザとユーザインタフェースの担当者とが、電話で“キャンセル”の処理を行なうことを合意し(音声通話500)、両者は、キャンセル操作を開始する。

【0189】ユーザインタフェースの担当者は、まず、モードスイッチ304で、クレジット決済増減300をクレジット決済モードに、図11 (a) の画面を表示させる。フアンクションスイッチ306で、図11 (b) の画面のように、メニューの中から“販売キャンセル”を選択し、実行スイッチ307を押す。すると、クレジット決済増減300には、図11 (c) の販売履歴一覧が表示され、担当者は、フアンクションスイッチ306で、図11 (d) の画面のように、キャンセルする取引を選択し、実行スイッチ308を押す。すると、図11 (e) の確認画面が表示され、担当者は、実行スイッチ308を押す(キャンセル操作901)。

【0190】すると、クレジット決済増減300は、サービス提供システム102に対して、“キャンセル”の処理を要求するメッセージ、キャンセル要求903を、デジタル無線通信によって送信する。この時、クレジット決済増減300は、図11 (f) の画面になる(キャンセル処理中表示902)。

【0191】一方、ユーザは、パーソナル・クレジット増減100を、モードスイッチ204でクレジットカードモードに、フアンクションスイッチ207で、LCD303に表示されるクレジットカードを切り替え、支払に使用済クレジットカードを選択する。さらに、フアンクションスイッチ207で、図10 (a) の画面に、フアンクションの中から“キャンセル”を選択し、実行スイッチ311を押す。すると、パーソナル・クレジット増減100には、図10 (b) の購入履歴一覧の画面が表示され、ユーザは、フアンクションスイッチ207で、キャンセルする取引を選択し、実行スイッチ311を押す。すると、図

(31)

10(c)の画面が表示され、ユーザは、実行スイ  
ッチ211を押す(キャンセル操作904)。

[0192] パーソナル・クレジット端末100は、サー  
ビス提供システム102に対して、“キャンセル”の処理  
を要求するメッセージ、キャンセル要求908を、デジタ  
ル無線電話通信によって送信する。この時、パーソナル  
・クレジット端末100は、図10(d)の画面を表示す  
る(キャンセル処理中905)。

[0193] サービス提供システム102は、クレジット  
決済端末300からのキャンセル要求908とパーソナル・ク  
レジット端末100からのキャンセル要求908とを、それぞ  
れ受信し、それらの内容を照合し、決済システム103に  
対して、“キャンセル”の処理を要求するメッセージ、  
キャンセル要求907を送信する。

[0194] 決済システム103は、サービス提供シス  
テム102からのキャンセル要求907を受信し、要求された取  
引のキャンセル処理を行ない、キャンセル処理が完了し  
たことを示すメッセージ、キャンセル完了通知908をサ  
ービス提供システム102に送信する。

[0195] サービス提供システム102は、決済シス  
テム103からのキャンセル完了通知908を受信し、クレジ  
ット決済端末300に、キャンセル処理が完了したことを示  
すメッセージ、キャンセル完了通知909をデジタル電話  
通信で送信し、さらに、パーソナル・クレジット端末10  
0に対して、キャンセル処理が完了したことを示すメッ  
セージ、キャンセル処理完了通知910を生成して、デジ  
タル無線電話通信で送信する。

[0196] クレジット決済端末300は、キャンセル完  
了通知を受信し、図11(g)のように、キャンセル完  
了通知の内容を表示して、キャンセル処理が完了したこ  
とを、担当者に知らせる(キャンセル処理完了表示91  
1)。

[0197] パーソナル・クレジット端末100は、キ  
ャンセル処理完了通知を受信し、図10(e)のように、キ  
ャンセル処理完了通知を表示して、キャンセル処理が完了  
したことを、ユーザに知らせる(キャンセル処理完了表  
示912)。

[0198] 以上のようにして、パーソナル・リモ  
ート・クレジット決済サービスの“キャンセル”の処理は行  
なわれる。このあと、担当者は、顧客サービスコールの  
操作(顧客サービスコール913)を行なうことによっ  
て、もう一度、ユーザと電話による通話(音声通話91  
4)をすることができ、顧客サービスコールについて  
は、この後、説明する。顧客サービスコールについて  
処理において、画面間で交換されるデータの詳細の詳  
細については、後で説明する。

[0199] 次に、“顧客サービスコール”の処理の流  
れを説明する。

[0200] 図12(a)は、パーソナル・リモート・  
クレジット決済サービスの“顧客サービスコール”の処

理の流れを示している。また、図13の(a)～(b)  
は、上記の“顧客サービスコール”の処理において、パ  
ーソナル・クレジット端末100のLCD303の表示例を示  
し、図14の(a)～(g)は、クレジット決済端末30  
0のLCD302の表示例を示している。

[0201] “顧客サービスコール”は、パーソナル・  
リモート・クレジット決済サービスの“決済”の処理に  
よって取引のあったユーザに対して、マーチャントがユ  
ーザの電話番号を知らない場合でも、電話連絡を可能に  
する処理である。したがって、“顧客サービスコール”  
は、ユーザとマーチャントとの間に、パーソナル・リモ  
ート・クレジット決済サービスの“決済”の処理による  
取引が、以前に、あったことが前提となる。

[0202] “顧客サービスコール”の処理は、マー  
チャントの担当者が、クレジット決済端末300で、“顧客  
サービスコール”の操作を開始するところから始まる。  
[0203] 図12(a)では、まず、マーチャントの  
担当者が、モディスイッチ304で、クレジット決済端末3  
00をクレジット決済モードにし、図14(a)の画面を  
表示させる。次に、担当者は、ファンクションスイッ  
チ305で、メニューの中から“販売履歴”を選択し、実行  
スイッチ308を押す。すると、クレジット決済端末300に  
は、図14(b)の販売履歴一覧が表示される。担当  
者は、ファンクションスイッチ305で、図14(c)の画  
面の右に、電話連絡しようとするユーザとの間で交  
わした取引を選択し、また、画面下の操作メニューか  
ら“電話”を選択し、実行スイッチ308を押す(顧客サ  
ービスコール操作1200)。すると、クレジット決済端  
末300は、自動的にデジタル電話モードになり、図14  
(d)の画面を表示し(接続処理中実行中表示1201)。  
サービス提供システム102に対して、“顧客サービスコ  
ール”の処理を要求するメッセージ、顧客サービスコ  
ール要求1202をデジタル電話通信によって送信する。

[0204] サービス提供システム102は、顧客サー  
ビスコール要求1202を受信し、ユーザが設定したアクセ  
ス制御情報と照合して、ユーザを呼び出すメッセージ、顧  
客サービスコール1203を、デジタル無線電話通信によ  
ってユーザのパーソナル・クレジット端末100へ送信す  
る。さらに、サービス提供システム102は、ユーザとの  
通話を許可するメッセージ、顧客サービスコール要求応  
答1204を、デジタル電話通信によって、クレジット決  
済端末300へ送信する。

[0205] クレジット決済端末300は、サービス提供  
システム102からの顧客サービスコール要求応答1204を  
受信し、図14(e)の画面を表示し、ユーザを呼び出  
していることを担当者に知らせる(呼び出し中表示120  
6)。

[0206] 一方、パーソナル・クレジット端末100  
は、顧客サービスコール1203を受信し、着信音を出  
し、図13(a)の画面を表示して、マーチャントから

(32)

電話が着信していることをユーザに知らせる(着信表示  
1205)。ユーザが通話スイッチ305を押すと(通話操作1  
207)、パーソナル・クレジット端末100は、ユーザが着  
信を受け入れたことを示すメッセージ、着信応答1208  
を、デジタル無線電話通信によってサービス提供シス  
テム102へ送信し、図13(b)の画面を表示する(通話  
中表示1209)。

[0207] サービス提供システム102は、着信応答120  
8を受信し、ユーザが呼び出しを受け入れたことを示す  
メッセージ、呼び出し応答1210を、デジタル電話通信に  
よって、クレジット決済端末300へ送信する。

[0208] クレジット決済端末300は、呼び出し応答1  
210を受信し、図14(f)の画面を表示し(通話中表  
示1211)。マーチャントは、ユーザと通話状態に入る  
(音声通話1212)。

[0209] 以上のようにして、パーソナル・リモート  
・クレジット決済サービスの“顧客サービスコール”の  
処理は行なわれる。

[0210] また、顧客サービスコールは、マーチャ  
ントの担当者が、図14(g)の販売履歴の詳細画面にお  
いて、画面下の操作メニューから“電話”を選択し、実  
行スイッチ308を押す(顧客サービスコール操作1200)  
ことによって、処理を開始することでもでき、また、図1  
1(g)の“キャンセル”の処理の完了画面において、  
画面下の操作メニューから“顧客サービスコール”を選  
択し、実行スイッチ308を押す(顧客サービスコール操  
作1200)ことによって、処理を開始することもできる。  
[0211] 上記の“顧客サービスコール”の処理にお  
いて、画面間で交換されるデータの内容の詳細について  
は、後で説明する。

[0212] 次に、“問い合わせコール”の処理の流れ  
を説明する。

[0213] 図12(b)は、パーソナル・リモート・  
クレジット決済サービスの“問い合わせコール”の処理  
の流れを示している。  
[0214] また、図13の(b)～(f)は、上記の  
“問い合わせコール”の処理において、パーソナル・ク  
レジット端末100のLCD303の表示例を示し、図14の  
(h)～(f)は、クレジット決済端末300のLCD302  
の表示例を示している。

[0215] “問い合わせコール”は、パーソナル・リ  
モート・クレジット決済サービスの“決済”の処理によ  
って取引のあったマーチャントに対して、ユーザが自分  
の電話番号を知られることなく、問い合わせの電話を可  
能にする処理である。

[0216] “問い合わせコール”の処理は、ユーザ  
が、パーソナル・クレジット端末100で、“問い合わせ  
コール”の操作を開始するところから始まる。

[0217] 図12(b)では、まず、ユーザが、モー  
ドスイッチ304で、パーソナル・クレジット端末100をク

レジットカードモードにし、図13(c)の画面を表示  
させる。次に、ユーザは、図13(d)の画面のよう  
に、ファンクションスイッチ207で、メニューの中から  
“利用履歴”を選択し、実行スイッチ211を押す。す  
ると、パーソナル・クレジット端末100には、図13  
(e)の販売履歴一覧が表示される。ユーザは、ファン  
クションスイッチ207で、図13(f)の画面のよう  
に、電話連絡しようとするマーチャントとの間で交わ  
した取引を選択し、また、画面下の操作メニューから  
“問い合わせ”を選択して、実行スイッチ211を押す  
(問い合わせコール操作1213)。すると、パーソナル・  
クレジット端末100は、自動的にデジタル無線電話モー  
ドになり、図13(g)の画面を表示し(接続処理中表  
行中表示1214)。サービス提供システム102に対して、  
“問い合わせコール”の処理を要求するメッセージ、問  
い合わせコール要求1215をデジタル無線電話通信によ  
って送信する。

[0218] サービス提供システム102は、問い合わせ  
コール要求1215を受信し、マーチャントを呼び出すメッ  
セージ、問い合わせコール1216を、デジタル電話通信に  
よってマーチャントのクレジット決済端末300へ送信す  
る。さらに、サービス提供システム102は、マーチャ  
ントとの通話を許可するメッセージ、問い合わせコール要  
求応答1217を、デジタル無線電話通信によって、パー  
ソナル・クレジット端末100へ送信する。

[0219] パーソナル・クレジット端末100は、サー  
ビス提供システム102からの問い合わせコール要求応答1  
217を受信し、図13(h)の画面を表示し、マーチャ  
ントを呼び出していることをユーザに知らせる(呼び出  
し中表示1219)。

[0220] 一方、クレジット決済端末300は、問い合  
わせコール1216を受信し、着信音を出し、図14  
(h)の画面を表示して、ユーザから電話が着信してい  
ることをマーチャントに知らせる(着信表示1218)。マ  
ーチャントの担当者が受話器303を取ると(通話操作122  
0)、クレジット決済端末300は、マーチャントが着信を  
受け入れたことを示すメッセージ、着信応答1221を、デ  
ジタル電話通信によってサービス提供システム102へ送  
信し、図14(f)の画面を表示する(通話中表示122  
2)。

[0221] サービス提供システム102は、着信応答122  
1を受信し、マーチャントが呼び出しを受け入れたこと  
を示すメッセージ、呼び出し応答1223を、デジタル無線  
電話通信によって、パーソナル・クレジット端末100へ  
送信する。

[0222] パーソナル・クレジット端末100は、呼び  
出し応答1223を受信し、図13(b)の画面を表示し  
(通話中表示1224)。ユーザは、マーチャントと通話状  
態に入る(音声通話1225)。  
[0223] 以上のようにして、パーソナル・リモート・

(33)

・クレジット保持サービスの“問い合わせコール”の処理は行はなれる。  
[0224] また、問い合わせコールは、ユーザが、図13(1)の利用履歴の詳細画面において、画面下の操作メニューから“問い合わせ”を選択し、実行スレッド21を押す(問い合わせコール操作113) ことによって、処理を開始することもできる。

[0225] 上記の“問い合わせコール”の処理において、検索部で検索されるデータの内容の詳細については、後で説明する。

[0226] 次に、パーソナル・クレジット端末1000内部の構成を説明する。

[0227] 図15(a)は、パーソナル・クレジット端末1000のブロック構成図である。この端末は、ROM(Read Only Memory)1501に格納されたプログラムにしたがって、送信データと受信データとの処理、及び、バス1539を介して他の構成要素の制御を行なうC P U (Central Processing Unit)1500と、C P U1500が処理するデータ、及びC P U1500が処理したデータが格納されるRAM(Random Access Memory)1502と、パーソナル・クレジット端末1000のターミナルID、電話番号、ユーザのユーザID、及びアライメント鍵と公開鍵、並びに、サービス提供システム102のサービス提供キーE P R O M (Electrically Erasable Programmable Read Only Memory)1503と、C P U1500の制御にしたがってLCD203の動作を制御し、C P U1500によって設定された画面をLCDに表示させるLCDコントローラ1504と、C P U1500の制御にしたがってデータの符号化処理及び復号化処理を行なう暗号処理プロセッサ1505と、C P U1500の復号化を行なうデータコデック1506と、赤外線通信の際に赤外線側の送信及び受信を行なう赤外線通信モジュール1507と、ユーザによるモードスイッチ204、通話スイッチ205、終了スイッチ206、フリップジョイスティック207、テンキースイッチ208、電源スイッチ209、及び実行スレッド211のスイッチ操作を検出するキー操作制御部1509と、スピーカ1510、レシーバ1512またはヘッドセットジャック213をドライブル、マイク210またはヘッドセットジャック213から入力するアナログ音声信号を増幅する音声処理部1511と、アナログ音声信号1540のアナログ音声データへの符号化とデジタル音声データのデコード処理部1543への復号化とを行なう音声コーデック1512と、無線チャネルにのる送信データの生成と受信データからの自分宛のデータの抽出とを行なうチャネルコーデック1513と、チャネルコーデック1513から入力されるシリアル・デジタル信号1547を、P L L1516から供給される発振電気信号1553をベースバンドとす、アナログ送信信号1549に変換する変調部1514と、P L L1516から供給される発振電気信号1553をアナログ受

信信号15500のベースバンドとしてアナログ受信信号1550を受信し、シリアル・デジタル信号1548をチャネルコーデック1513へ供給する復調部1515と、変調部1514から供給されたアナログ送信信号1549を無線電波に変えてアンテナ1516から出力し、逆に、無線電波をアンテナ201が受信すると、復調部1515にアナログ受信信号1550を入力するR F部1517と、パーソナル・クレジット端末1000のパーソナルの容量を検出するパーソナル容量検出部1518と、チャネルコーデック1513、P L L1516及びR F部1517の起動制御、キー操作制御部1509、チャネルコーデック1513及びアンテナ1516の容量検出部1518から入力する割り込み信号の処理、並びに、C P U1500がキー操作制御部1509、音声処理部1511及びチャネルコーデック1513の内部のレジスタをアクセスする際、インターフェースの役割を果たす制御ロジック部1508とを備えている。

[0228] 暗号処理プロセッサ1505は、秘密鍵方式の符号化及び復号化の際に公開鍵方式の符号化及び復号化の機能とをもち、C P U1500によって設定された暗号方式と鍵とで、C P U1500によって設定されたデータを暗号化処理または復号化処理する。

[0229] また、データコデック1506は、C P U1500の制御にしたがって送信データの符号化及び受信データの復号化を行なうが、この場合の符号化とは、通信制御情報、割り訂正情報を含んだ、実際に送信されるデータを生成する処理を意味し、復号化とは、受信データに対し、割り訂正処理を施し、余分な通信制御情報を取り除き、本来、送り手が送信しようとしたデータを生成する処理を意味する。データコデック1506は、デジタル無線電話のデータ通信におけるデータの符号化及び復号化の機能と、赤外線通信におけるデータの符号化及び復号化の機能とをもち、C P U1500によって設定されたデータに対して、C P U1500によって設定された符号化処理及び復号化処理を行なう。

[0230] また、赤外線通信モジュール1507は、図15(b)に示すように、その内部に、パルスデータとシリアルデータとの両方向の変換を行なう直列-並列変換回路1560と、直列-並列変換回路1560によってシリアルデータに変換されたデジタル信号1562を復調し、赤外線として送信される信号に変換し、また、受信したアナログ信号1565をシリアル・デジタル信号1563に変換する変復調回路1561と、変換回路1561によって変換された信号1564を赤外線に変換して発光し、また、受光した赤外線をアナログ信号1565に変換する赤外線受光部1508とを具備している。

[0231] また、ユーザによるスイッチ操作を検出するキー操作制御部1509は、ユーザが、モードスイッチ204、通話スイッチ205、終了スイッチ206、フリップジョイスティック207、テンキースイッチ208、電源スイッチ209または実行スレッド211のいずれかを押すと、キー操作制御部1509は、C P U1500に、スイッチ操作に対応する

処理を促す割り込み信号1538をスタートする。また、キー操作制御部1509は、図18(a)に示すように、各スレッドの有効/無効を設定するキー操作制御レジスタ(ECT)1812を具備している。  
[0232] また、音声処理部1511は、図18(a)に示すように、音声処理動作を制御する音声処理部制御レジスタ(SCIT)を具備している。

[0233] また、音声コーデック1512は、音声処理部1511から入力するアナログ音声信号1542のデジタル音声データへの符号化と、チャネルコーデック1513から入力するデジタル音声データのアナログ音声信号1543への復号化とを行なう。アナログ音声信号1543は、音声処理部1511へ供給され、音声処理部1511が、アナログ音声信号1543を増幅し、レシーバ1512をドライブルすることによって、レシーバ1512から音声出力される。また、符号化によって生成されたデジタル音声データは、チャネルコーデック1513へ供給され、実際に、無線チャネルにのる送信データに変換される。

[0234] また、チャネルコーデック1513には、送信するデータとして、二重頭のデータが入力される。一つは、音声コーデック1512から入力するデジタル音声データであり、もう一つは、C P U1500から、制御ロジック部1508を介して、入力するデータ通信データである。  
[0235] チャネルコーデック1513は、デジタル音声データとデータ通信データとの識別情報、ヘッダ情報として、それぞれのデータに付加し、さらに、デジタル無線電話のデータコデック1506に変換して、シリアル・デジタル信号1547を、変調部1514へ供給する。

[0236] その逆に、チャネルコーデック1513は、復調部1515から入力するシリアル・デジタル信号1548に対して、まず、ターミナルIDを照合して、自分宛のデータのみの抽出し、さらに、デジタル無線電話の通信制御情報を取り除き、データのヘッダ情報から、デジタル音声コーデック1512と制御ロジック部1508とへ供給する。また、チャネルコーデック1513は、デジタル無線電話を増幅した時と、データ通信データを受信した時とに、割り込み信号1554をスタートする。割り込み信号1554は、C P U1500に、デジタル無線電話の着信時の処理と、データ通信データの処理とを促す割り込み信号である。

[0237] チャネルコーデック1513は、こうした動作を行なうために、図18(a)に示すように、ターミナルIDを格納する1Dレジスタ(1D)1805と、チャネルコーデック1513の動作を制御するチャネルコーデック制御レジスタ(CNCT)1806と、音声コーデック1512から入力されるデジタル音声データを格納する音声送信バッファ1807と、受信データの中から抽出したデジタル音声データを格納する音声受信バッファ1808と、制御ロジック部1508から入力されるデータ通信データを格納する

データ送信バッファ1809と、受信データの中から抽出したデータ通信データを格納するデータ受信バッファ1810とを具備している。  
[0238] 変調部1514は、チャネルコーデック1513から入力するシリアル・デジタル信号1547を、P L L1516から供給される発振電気信号1553をベースバンドとするアナログ送信信号1549に変換し、R F部へ供給する。R F部へ供給されたアナログ送信信号1549は、無線電波として、アンテナ201から出力される。

[0239] 逆に、無線電波をアンテナ201が受信すると、R F部1517から復調部1515にアナログ受信信号1550が入力される。復調部1515は、P L L1516から供給される発振電気信号1553を、アナログ受信信号15500のベースバンドとして、アナログ受信信号1550を復調して、シリアル・デジタル信号1548を、チャネルコーデック1513へ供給する。

[0240] また、パーソナル容量を検出するパーソナル容量検出部1518は、パーソナル・クレジット端末1000のパーソナルの容量が、C P U1500によって設定された値Q (Q>0) 以下になった時に、割り込み信号1557をスタートする。割り込み信号1557は、C P U1500にRAM1502上のデータのバッファアツク処理を促す割り込み信号であり、Qは、パーソナル・クレジット端末1000がバッファアツク処理を行なうのに十分な値である。  
[0241] また、制御ロジック部1508は、図18(a)に示すように、その内部に、フレームカウンタ(FRAME)1800、起動フレームレジスタ(FRAME)1801、クロックカウンタ(CLOCK)1802、フリップデータ時刻レジスタ(PRTIME)1803、及び割り込みレジスタ(INT)1804の5つのレジスタを内蔵する。

[0242] フレームカウンタ1800は、デジタル無線電話のフレーム数をカウントするカウンタ。起動フレームレジスタ1801は、次の起動するフレーム番号を格納するレジスタ。クロックカウンタ1802は、現在の時刻をカウントするカウンタ。フリップデータ時刻レジスタ1803は、パーソナル・クレジット端末1000が、サービス提供システム102と通信して、RAM1502上のデータを更新する処理(フリップデータ処理)を行なう時刻を格納するレジスタ。そして、割り込みレジスタ1804は、C P U1500への割り込みの要因を示すレジスタである。

[0243] 一般に、デジタル無線電話では、デジタル無線電話の制御チャネルの制御データを周期的に受信し、ターミナルIDと照合することによって、自分宛の電話の着信を提示している。このパーソナル・クレジットの端末1000では、フレームカウンタ1800と起動フレームレジスタ1801とを用いて、制御データの間の受信を行なう。すなわち、起動フレームレジスタ1801に、次に起動するフレーム番号を格納しておき、フレームカウンタ1800がカウントアップして、起動フレームレジスタ1801の値に等しくなった時、制御ロジック部1508が、アドレス

(34)

データ番号1558を介して、チャンネルコードデック151  
3、PLL1516、及びRF部1517を起動し、制御データ  
の受信を行なう。

[0 2 4 4] また、制御ロジック部1508は、割り込み番  
号1538、1554、1557のいずれかの割り込み番号がサート  
されると、その割り込み要因を、割り込みレジスタ(C  
T)1804に設定して、割り込み番号1519をアサートし、  
PUI1500に割り込み処理を促す。CPU1500は、割り込  
み処理で、割り込みレジスタ1804を読み出し、その割り  
込み要因に応じた処理を行なう。

[0 2 4 5] この割り込みレジスタ(INT)1804の各ビ  
ットフィールドは、図18 (b) に示すように意味づけら  
れている。

[0 2 4 6] ビット231は、電源スイッチ209の状態を  
示し、値が0の時、パワーオフの状態であることを示  
し、値が1の時、パワーオン状態であることを示す。

[0 2 4 7] ビット30は、デジタル無線電話通信の状  
態を示し、値が0の時、デジタル無線電話通信をしてい  
ない状態であることを示し、値が1の時、デジタル無線  
電話通信をしている状態であることを示す。

[0 2 4 8] ビット29は、制御データの周次受信を促  
すフレイム割込の発生を示し、値が1の時、フレイム割  
込が起こったことを示す。このビットフィールドには、  
フレイムカウンタ1800の値が、起動フレイムレジスタ18  
01の値に一致した時に、1が設定される。

[0 2 4 9] ビット28は、着信割込の発生を示し、値  
が1の時、デジタル無線電話を着信したことを示す。こ  
のビットフィールドには、デジタル無線電話の制御デー  
タの周次受信において、タumerナルIDが一一致し、割り  
込み番号1554がアサートされた時に、1が設定される。

[0 2 5 0] ビット27は、データ受信割込の発生を示  
し、値が1の時、データ受信データを受領したことを示  
す。このビットフィールドには、デジタル無線電話通信  
において、データ通信データを受信し、割り込み番号15  
54がアサートされた時に、1が設定される。

[0 2 5 1] ビット26は、データアップ処理を  
促すアップデータ割込の発生を示し、値が1の時、アッ  
プデータ割込が起こったことを示す。このビットフィー  
ルドには、クロックカウンタ802の値が、アップデータ  
時刻レジスタ803の値に一致した時に、1が設定され  
る。

[0 2 5 2] ビット25は、バックアップ処理を促すバ  
ッテリ割込の発生を示し、値が1の時、バッテリ割  
込が起こったことを示す。このビットフィールドには、  
バッテリ電量検出部1518から入力する割り込み番号15  
57がアサートされた時に、1が設定される。

[0 2 5 3] ビット24は、スイッチ操作によるキー割  
込の発生を示し、値が1の時、キー割込が起こったこと  
を示す。

[0 2 5 4] また、ビット0からビット9は、それぞ

れ、デンキスイッチ208の0から9のスイッチに対応  
し、ビット10とビット11とは、それぞれ、デンキ  
スイッチの“\*”と“#”とのスイッチに対応し、ビッ  
ト12からビット15は、それぞれ、ファンクション  
スイッチ207の“F1”から“F4”のスイッチに対応し、ビ  
ット16からビット20は、それぞれ、電源スイッチ20  
9、実行スイッチ211、モーススイッチ204、画面スイッ  
チ205、終了スイッチ206に対応し、ビットの値が1の  
時、そのビットに対応するスイッチが押されたことを示  
す。

[0 2 5 5] 次に、RAM1502に格納されるデータに關  
して説明する。

[0 2 5 6] 図16は、RAM1502に格納されるデータ  
のRAMマップの模式図である。

[0 2 5 7] RAM1502には、基本プログラム領域160  
0、サービスデータ領域1601、ユーザ領域1602、ワーク  
領域1603、及びテンポラリ領域1604の五つの領域があ  
る。基本プログラム領域1600は、ROM1501に格納され  
ているプログラムのバージョンアップされたモジュ  
ール、及び、パッチプログラムが格納される。

[0 2 5 8] ユーザ領域1602は、ユーザが自由に使用で  
きる領域、ワーク領域1603は、CPU100がプログラ  
ムを実行する際に使用する作業領域、また、テンポラリ領  
域1604は、パーソナル・クレジットカード100が受信した  
情報を一時的に格納する領域である。サービスデータ領  
域1601は、パーソナル・リモート・クレジット決済サ  
ービスのID情報や、クレジットカード情報、履歴情報な  
どを格納する領域であり、この領域のデータは、サービ  
ス提供システム102によって管理される。

[0 2 5 9] サービスデータ領域1601には、さらに、デ  
ータ管理情報1605、個人情報1606、写真データ1607、ユ  
ーザ設定情報1608、電話情報1609、クレジットカー  
ド1610、利用履歴リスト1611、及び実態データ領域16  
12の8つ領域がある。データ管理情報1605は、サービ  
スデータ領域1601に格納されている情報の管理情報を格納  
する領域、個人情報1606は、ユーザの名前、年齢、性別  
等の情報を格納する領域、写真データ領域1607は、ユ  
ーザの顔写真のデータを格納する領域、ユーザ設定情報16  
08は、パーソナル・リモート・クレジット決済サ  
ービスに関する、ユーザの設定情報を格納する領域、電話情報  
1609は、デジタル無線電話に関連する情報を格納する領  
域、クレジットカード1610は、ユーザが登録した  
クレジットカードのリスト情報を格納する領域、利用履  
歴リスト1611は、パーソナル・リモート・クレジット決  
済サービスの利用履歴情報を格納する領域、実態データ  
領域1612は、他の7つの領域で管理されている情報の実  
体データを格納する領域である。

[0 2 6 0] 次に、サービスデータ領域1601に格納され  
る情報について詳しく説明する。

[0 2 6 1] 図17は、サービスデータ領域1601に格納

される情報の関係を詳細に表した模式図である。

[0 2 6 2] データ管理情報1605は、アップデータ日時  
1700、次回アップデータ日時1701、ターミナル・ステイ  
タス1703、個人情報1708、写真データアドレス  
1704、ユーザ設定情報アドレス1705、電話情報アドレス  
1706、クレジットカードリスト・アドレス1707、及び利  
用履歴リスト・アドレス1708の9つの情報によって構成  
される。

[0 2 6 3] アップデータ日時1700は、サービス提供シ  
ステム102が、前回、サービスデータ領域1601のデータ  
を更新した日時を示し、次回アップデータ日時1701は、  
次回のサービス提供システム102によるサービスデー  
タ領域1601のデータの更新の予定日時を示す。パーソナル  
・クレジット端末100は、次回アップデータ日時1701の  
設定された時間になると、自動的に、データアップデー  
タ処理を開始する。

[0 2 6 4] データアップデータ処理は、サービス提供  
システム102に、サービスデータ領域1601のデータを更  
新してもらう処理である。データアップデータ処理につ  
いては、後で詳しく説明する。

[0 2 6 5] ターミナル・ステイタス1703は、パーソ  
ナル・クレジット端末100の状態を示し、個人情報アド  
レス1703、写真データアドレス1704、ユーザ設定情報アド  
レス1705、電話情報アドレス1706、クレジットカードリス  
ト・アドレス1707、及び利用履歴リスト・アドレス17  
08は、それぞれ、個人情報1606、写真データ1607、ユ  
ーザ設定情報1608、電話情報1609、クレジットカードリス  
ト1610、利用履歴リスト1611が格納されている領域の先  
頭番地を示す。

[0 2 6 6] 電話情報1609は、さらに、発信電話番号17  
09、電話機アドレス1710、短縮ダイヤル設定ファイル・  
アドレス1711の3つの情報によって構成される。発信電  
話番号1709は、ユーザが、前回、かけた電話の電話番号  
を示し、この情報は、デジタル無線電話の再発時に用い  
られる。電話機アドレス1710は短縮ダイヤル設定ファイ  
ル・アドレス1711とは、それぞれ、電話機情報、短縮ダ  
イヤル設定ファイルが格納されている実体データ領域上  
のアドレスを示す。

[0 2 6 7] クレジットカードリスト1610には、ユーザ  
が登録したクレジットカードのリスト情報が格納されて  
いる。クレジットカードリスト1610では、一つのクレジ  
ットカードに対して、クレジットカード名1712(1719)、  
クレジットカード番号1713(1720)、有効期限1714(172  
1)、クレジットカード・ステイタス1715(1722)、イメ  
ージ・データ・アドレス1716(1723)、オブジェクト・デ  
ータ・アドレス1717(1724)、及びアクセス時刻1718(1725)  
の7つの情報が格納されている。

[0 2 6 8] クレジットカード・ステイタス1715(1722)  
は、クレジットカードが有効か否か、及び、利用限度額  
を示し、イメージ・データ・アドレス1716(1723)は、ク

レジットカードのイメージデータが格納されている実体  
データ領域1612上のアドレスを示す。オブジェクト・デ  
ータ・アドレス1717(1724)は、そのクレジットカードの  
プログラムのオブジェクト・データが格納されているア  
ドレスを示し、アクセス時刻1718(1725)は、ユーザがそ  
のクレジットカードを利用した最後の時刻を示す。

[0 2 6 9] オブジェクト・データ・アドレス1717(172  
4)には、実体データ領域1612上のアドレスを示すローカ  
ルアドレス、または、サービス提供システム102のユー  
ザ情報サーバ1402上のアドレスを示すリモートアドレ  
スが格納される。オブジェクト・データ・アドレス1717(1  
724)に、リモートアドレスが格納されている場合、ユー  
ザが、そのクレジットカードを選択し、利用しようとし  
ると、パーソナル・クレジット端末100は、サービス提  
供システム102から、オブジェクト・データをデメンボラ  
リ領域1604にダウンロードし、クレジットカードのプロ  
グラムを実行する。クレジットカードを表示するだけで  
は、イメージ・データ・アドレス1716(1723)によって示  
される実体データ領域1612のイメージデータが表示さ  
れ、オブジェクト・データのダウンロードは行なわ  
ない。

[0 2 7 0] オブジェクト・データ・アドレス1717(172  
4)に格納されるアドレスは、サービス提供システム102  
によって決定される。データアップデータ処理の際に、  
各クレジットカードのアクセス時刻を比較し、アクセス  
時刻が最近のクレジットカードに、ローカルアドレスが  
割り当てられる。但し、実体データ領域1612の番地に余  
裕がある場合には、全てのクレジットカードのオブジェ  
クト・データ・アドレスが、ローカルアドレスである場  
合もある。

[0 2 7 1] 利用履歴リスト1611では、一つのパーソ  
ナル・リモート・クレジット決済サービスの利用に対し  
て、要求番号1725(1730)、サービスコード1727(1731)、  
利用時刻1728(1732)、及び利用情報アドレス1729(1733)  
の4つの情報が格納される。

[0 2 7 2] 要求番号1725(1730)は、マーチャントとの  
取引をユニークに示す番号であり、支払オフア608を  
生成する際に、パーソナル・クレジット端末100が発行  
する番号、サービスコード1727(1731)は、利用したクレ  
ジットカードサービスの種類を示すコード番号、利用時  
刻1728(1732)は、パーソナル・リモート・クレジット決済  
サービスを利用した時刻、利用情報アドレス1729(1733)  
は、収銀書が格納されているアドレスを示す。

[0 2 7 3] 利用情報アドレス1729(1733)には、実体デ  
ータ領域1612上のアドレスを示すローカルアドレス、ま  
たは、サービス提供システム102のユーザ情報サーバ1402  
上のアドレスを示すリモートアドレスが格納される。

[0 2 7 4] 利用情報アドレス1729(1733)に、リモート  
アドレスが格納されている場合、ユーザが、その利用履  
歴情報をアクセスすると、パーソナル・クレジット端末、



1001は、サービスタップシステム103から、利用情報をデンプラリ領域1604にダウンロードして、LCD203に表示する。

〔0275〕利用情報アドレス1729(1733)に格納されるアドレスもまた、サービスタ提供システムによって決定される。データアクセス時に処理の際に、各利用情報の利用時刻を比較し、利用時刻が近隣の順に各情報に対して、ローカルアドレスが割り当てられる。但し、媒体データアクセス16120の容量に余裕がある場合には、全ての利用情報アドレスが、ローカルアドレスである場合もある。

【0276】次に、CPU1500が行なう処理について説明する。

【0277】図19は、CPU1500が行なう処理のフローチャートである。

【02278】 函19に示すように、CPU1500の処理は、大きく分けて、10種類のプロセスと、割込処理1901とに分けることが出来る。

せる、無線電話ブローセス、クレジットカードブローセス、  
[02719] 10種類のブローセスとは、パワーオンブロー  
セス、無線電話ブローセス、顧客サービスコンピュータブ  
ロセス、データベースブローセス、バックアップブローセ  
ス、リモートアクセスブローセス、セクション独立ブロー  
セス、及びパワーオンブローセスであり、この10種類のブ

【0280】各プロセスには、そのプロセスに対応して、プロセスのステータス（状態）を示すワードワイヤがRAM1502上に存在し、CPU1500は、このプロ

セススデイトナスの値に応じて、各プロセスを実行する。  
 (02811) パワーオンプロセスは、ユーザが電話ス  
 イッチをオンした時の初期動作処理を行なうプロセス、無  
 線電話プロセスは、デジタル無線電話モード時の処理を  
 行なうプロセス、クレジットカードプロセスは、クレジ

ットカードモード時の処理を行なうプロセス、問い合わせコールプロセスは、「問い合わせコール」の処理を行なうプロセス、顧客サービスコールプロセスは、「顧客サービスコール」の処理を行なうプロセス、データアップ

フヂー・トロセスとは、データフッヂー処理を行なうフロッピー、バックアップフロッピーとは、バックアップ処理を行なうフロッピー、リモートアクセス上のデータは、サブシステムの入システムのユーザ制御システム上のデータは、サブシステムを処理を行なうフロッピー、セクション独立アクセスは、ユーザ提供システムとの通信セクションを形成する処理を行なうフロッピー、パワートロセスとは、ユーザが電源スイッチをオフした時の終了処理を行なうフロッピーである。

【0282】図19において、パーソナル・クレジット端末をリセットすると、ステツァ1902へ進み、CPU1001は、パワーオンプロセスを“active”にする。

が“active”か否かを調べ、“inactive”の場合、ス

テツゾ1905へ進み、“active”の場合は、ステツゾ190へ進み、パワーオンプロセスを一定時間実行して、ステツゾ1905へ進む。

【0284】ステツパ1905では、無線電話フロセスが“active”か否かを調べ、“inactive”の場合は、スラツパ1907へ進み、“active”の場合は、ステツパ1906へ進み、無線電話フロセスを一定時間実行して、ステツパ1907へ進む。

【0285】ステツア1907では、クレジットカードアセスが“active”か否かを調べ、“inactive”の場合は、ステツア1909へ進み、“active”の場合は、ステツア1908へ進み、クレジットカードアセスを一定時間実行

行して、ステツツ1809へ進む。ステツツ1809では、問い合わせコールプロセスが“active”か否かを調べ、“active”の場合は、ステツツ1911へ進む。“active”の場合は、ステツツ1910へ進む。問い合わせコールプロセスを一定時間実行して、ステツツ1911へ進む。ステツツ1911へ進む。

1911 年には、顧客サービススコアプロセスが "active" な否かを調べ、"inactive" の場合は、ステータス1913へ進み、"active" の場合は、ステータス1912へ進み、顧客サービススコアプロセスを一定時間実行して、ステータス1913へ進む。

【0286】ステツァ1915では、データツァデートロセ入が“active”か否かを問へ、“inactive”の場合は、ステツァ1915へ進み、“active”の場合は、ステツァ1914へ進み、データツァデートロセ入を一定時間実行して、ステツァ1915へ進む。

【0287】ステツァ1915では、バックアツツアロセが“active”か否かを問へ、“inactive”の場合は、ステツァ1917へ進む、“active”の場合は、ステツァ1918へ進む、バックアツツアロセを一定時間実行して、ステツァ1917へ進む。

【02088】スレッツ1917では、リモートアクセスでは、"active"が"否かを問へ、"inactive"の場合は、スレッツ1919へ進み、"active"の場合は、スレッツ1918へ進み、リモートアクセスを一定時間

行して、ステツジ1919へ進む。ステツジ1919では、セ  
ション確立プロセスが“active”か否かを問へ、“in  
live”の場合は、ステツジ1921へ進む、“active”の  
場合は、ステツジ1920へ進む、セツション確立プロセ  
ス一定時間実行して、ステツジ1921へ進む。

【0289】ステツァ1921では、ハローオプアロセス  
“active” か否かを問へ、“active” の場合、ステツ  
1922へ進み、ハローオプアロセスを実行し、“inactive”  
e”の場合は、ステツァ1903へ戻る。CPUは、割り込

み番号1518がアサートされると、割込処理1901を実行し、元のメインループ1900の処理に戻る。

【0290】割込処理1901では、まず、CPU1500はステッパ1932で、割り込みレジスタ(INT)1804を読みだし、RAM（ワーク領域）上のワーキ interruppl にコピー

一する。この時、CPUに提供された割り込みレシ  
タ(INT)1804は、エコーリセットされる。  
【0291】次に、ステツァ1924で、interruptのどッ

ト288の頃から、着信割込が音かを聞く、着信割込でない場合 (Interrupt (b)128)=0)、ステツツ1926へ進み、着信割込の場合 (Interrupt (b)128)=1)は、ステツツ1925へ進み、無線電話プロセスのプロセスステイタスを“active”にして、ステツツ1926へ進む。

【0292】スチツプ156では、interruptのビット2  
6の値から、アツチード割込か否かを調べ、アツチード  
割込でない場合 (interrupt (b1126)=0)、スチツプ1  
28に進み、アツチード割込の場合 (interrupt (b1126)

1)は、ステツク1927へ進み、チークツクチートノロで  
スのプロセスステイタスを“active”にして、ステツク  
1928へ進む。

【0293】ステツク1924では、Interruptのビット2  
5の値から、バックアップ割込み番を調べ、バックアップ

ツテ割でない場合 (InErrorP (b) i 25 = 0)、ステツツ  
30へ進み、バツクアツテ割の場合 (InErrorP (b) i 25)  
1)は、ステツツ1939へ進み、バツクアツテ割セオのフ  
ロセスステイタスを “active” にして、ステツツ1930へ  
進む。

4の値から、キー割込が否かを調べ、キー割込でない場合は (Interrupt (b) (24) = 0)、割込処理を終了し、元のメインループの処理へ戻り、キー割込の場合 (Interrupt (b) (24) = 1) は、ステップ1931へ進む。

【0295】スレッツ1931では、Interruptの「電圧ビット」(b1116)の値を調べ、0の場合は、割込処理を終了し、元のメインループの処理へ戻り、1の場合は、電圧スレッツが操作されたと判定し、スレッツ1932へ進む。

「表示」ビット(b11131)の値を調べ、0の場合には、パワー  
オフの操作が行なわれたと判定し、ステツア1934へは  
み、1の場合には、パワーオフの操作が行なわれたとき

【0297】ステツア1933では、パワーオンプロセスの  
プロセスステータスを“active”にして、割込処理を  
し、元のメインループの処理へ戻る。  
【0298】ステツア1934では、パワーオフプロセス

プロセステイタスに“active”にして、割込処理を  
し、元のメイソループの処理へ戻る。  
【0299】割込処理101の中で、プロセステイタ  
スが“active”になったプロセスは、メイソループに戻

り、メイクループの中で実行される。

【03001】次に、パーソナル・クレジット端末が、メイクループの終了を知らせる。このメッセージは、メイクループの開始時に送信されたメッセージと対応する。このメッセージは、メイクループの終了時に送信される。このメッセージは、メイクループの終了時に送信される。

10301 ナンタル 著石処理と封鎖に処理には、シ  
ット決済端末でも同様の処理を行なうので、以下で  
は、登場人物は、ユーザ、マシーナント、サービス提供

登場人物を一般化して説明する。

〔0302〕デジタル署名は、公開鍵方式の符号化処理の「プライベート鍵で暗号化したメッセージは、その「プライベート鍵に対応する公開鍵でしか復号化できない」

す処理である。

【0303】図20(a)、(b)は、それぞれ、メッセージ(Message)に、Aさんのデジタル署名をする場合

【0304】まず、ステップ2000で、CPUは、メッセージ2003に対して、ハッシュ関数演算を行い、メッセージ・ダイジェスト2004を生成する。

【0305】次に、ステップ2001で、CPUは、デジタルプロセスを用いて、メッセージ・ダイジェスト2004を、Aさんのプライベート鍵で暗号化して、デジタルサイン2005を生成する。

上の手順によって、CPUは、Aさんのデジタル署名をしたメッセージ2006を生成する。

【0307】図20(b)の2006は、Aさんのデジタル署名をしたメッセージを图示したものであり、以下で

は、デジタル署名されたメッセージは、図面の中ではない。2006のように、図示することとする。

【0308】次に、封鎖化処理について説明する。封鎖化処理は、公開鍵方式の暗号化処理の「公開鍵で暗号化したメッセージは、その公開鍵に対応するプライベート

【030309】図21(a)、(b)は、それぞれ、Aさ  
である。

んのデジタル署名をしたメッセージを、送り先のBさん宛に封書化する処理の手順を示すフロー図と、フロー図の概念解説図である。

【0310】まず、ステップ100で、CPUは、ランダム関数を用いて、秘密鍵方式の暗号鍵、秘密鍵210を生

成する。次に、ステツツア2101で、C P Uは、暗号処理ソフトウェアを用いて、デジタル署名をしたメッセージ2000を、秘鍵2104で暗号化する。

型ノビデワツテを用いて、板厚210μを返り元のままに  
公認検定暗号化する。

(0 3 1 2) 次に、ステツプ2103で、CPUは、ステツ  
プ2101の出力2105に、ステツプ2102の出力2106を付加す  
る。以上の手順によって、Bさん宛に封鎖化されたメッ

セージ2107を生成する。

[0 3 1 3] 図 2 1 (b) の2007は、Bさん宛に、封書化されたメッセージを宛示したものであり、以下では、封書化されたメッセージは、図面の中では、2007のようになり、図示することとする。

[0 3 1 4] 次に、パーソナル・クレジット端末が、サービス提供システムからメッセージを受信した際に、デジタル封書化されたメッセージの暗号の復号化処理と、デジタル署名名の検証処理について説明する。この場合でも、登場人物は一般化して説明する。

[0 3 1 5] まず、復号化処理について説明する。

[0 3 1 6] 図 2 2 (a)、(b) は、それぞれ、Bさん宛に封書化されたメッセージの復号化処理の手順を示すフロー図と、フローの概念解説図である。

[0 3 1 7] まず、ステップ2207で、CPUは、Bさん宛に封書化されたメッセージ2207を、秘密鍵をBさんの公開鍵で暗号化した部分2203と、秘密鍵で暗号化されたメッセージの部分2204とに分け、暗号処理プロセスを用いて、秘密鍵をBさんの公開鍵で暗号化した部分2203を、Bさんのプライベート鍵で復号化し、秘密鍵2205を取り出す。

[0 3 1 8] 次に、ステップ2207で、CPUは、暗号処理プロセスを用いて、秘密鍵で暗号化されたメッセージの部分2204を秘密鍵2205で復号化する。

[0 3 1 9] 以上の手順によって、封書化されたメッセージの復号化を行う。

[0 3 2 0] 次に、デジタル署名名の検証処理について説明する。

[0 3 2 1] 図 2 3 (a)、(b) は、それぞれ、メッセージの送り手のAさんのデジタル署名名がされたメッセージのデジタル署名名の検証処理の手順を示すフロー図と、フローの概念解説図である。

[0 3 2 2] まず、ステップ2307で、CPUは、デジタル署名名がされたメッセージ2306の中のメッセージの部分2308と、ハッシュ関数演算を行ない、メッセージ・ダイジェスト2305を生成する。

[0 3 2 3] 次に、ステップ2307で、CPUは、暗号処理プロセスを用いて、デジタル署名名がされたメッセージ2306の中のデジタルサインの部分2304を、Aさんの公開鍵で復号化する。

[0 3 2 4] 次に、ステップ2307で、CPUは、ステップ2308の出力2301の出力2304とを比較し、内容が一致した場合、検証をパスしたと判定し、一致しなかった場合、検証エラーが発生したと判定する。

[0 3 2 5] 以上の手順によって、デジタル署名名の検証処理を行う。

[0 3 2 6] 次に、クレジット決済端末300の内部の構成を説明する。

[0 3 2 7] 図 2 4 (a) は、クレジット決済端末300のブロック構成図である。この端末300は、ROM (Read

Only Memory) 2401に格納されたプログラムにしたがって、送信データと受信データの処理、及びバス2439を介して他の構成要素の制御を行なうCPU (Central Processing Unit) 2400と、CPU 2400が処理するデータ及びCPU 2400が処理したデータが格納されるRAM (Random Access Memory) 2402と、RAM 2402上のデータの管理情報によって指定された情報の実体データが格納されるハードディスク2403と、クレジット決済端末300のターミナルID、電話番号、マーチャントのマーチャントID、プライベート鍵及び公開鍵、並びに、サービス提供システム102のサービス提供者ID、電話番号、及びサービス提供者の公開鍵が格納されるEEPROM (Electric Erasable Programmable Read Only Memory) 2404と、CPU 2400の制御にしたがってLCD 202の動作を制御し、CPU 2400によって設定された画面をLCD 202に表示させるLCDコントローラ2405と、CPU 2400の制御にしたがってデータの暗号化処理及び復号化処理を行なう暗号処理プロセス2406と、CPU 2400の制御にしたがって、送信データの符号化及び受信データの復号化を行なうデジタルコーデック2407と、シリアルポート2409を介してシリアルケーブル310で赤外線モジュール301と接続し、パラレルデータとシリアルデータとの両方の変換を行なう直列-並列変換回路2408回路と、マーチャントによるモジュール304、フックスイッチ305、ファンクションスイッチ306、テンキースイッチ307、実行スイッチ308または電源スイッチ309のスイッチ操作を検出して割り込み信号2439をアサするキーボード制御部2411と、スピーカ2412と受話器303のレシーバログ音声信号を増幅する音声処理部2413と、アナログ音声信号2444のデジタル音声データへの符号化とデジタル音声データのデジタル音声信号2443への復号化とを行なう音声データのデジタル音声信号2443をデジタル音声データに復号化する音声処理部2414と、通信チャネルに乗る送信データの生成と受信データからのデジタル音声データ及びデータ通信データの分別とを行なうチャネルコーデック2415と、デジタル信号2448をデジタル電話通信のデータフォーマットに変換し、また、その逆変換をするデジタル通信アダプタ2416と、RS-232Cケーブル2413を接続するRS-232Cインターフェイス2417と、キーボード制御部2411、チャネルコーデック2415またはRS-232Cインターフェイス2417から入力する割り込み信号の処理、及び、CPU 2400がキーボード制御部2411、音声処理部2413またはチャネルコーデック2415の内部のレジスタをアクセスする際のインターフェースの役割を果たす制御ロジック2410とを備えている。

[0 3 2 8] 暗号処理プロセス2406は、秘密鍵方式の暗号化及び復号化と、公開鍵方式の暗号化及び復号化とを備え、CPU 2400によって設定された暗号方式と鍵と、CPU 2400によって設定されたデータを、暗号化処理または復号化処理する。

[0 3 2 9] また、データコーデック2407は、CPU 2400の制御にしたがって、送信データの符号化と受信データの復号化とを行なうが、この場合の符号化とは、通信制御情報、割り込み信号を含んだ、実際に送信されるデータとを生成する処理を意味し、復号化とは、受信データに対し、割り込み信号を抽出し、余分な通信制御情報を取り除き、本来、送り手が送信しようとしたデータを生成する処理を意味する。データコーデック2407は、デジタル電話のデータ通信におけるデータの符号化及び復号化の機能と、赤外線通信におけるデータの符号化及び復号化の機能とをもち、CPU 2400に設定されたデータに対して、CPU 2400に設定された符号化処理及び復号化処理を行なう。

[0 3 3 0] また、シリアルケーブル310及びシリアルポート2409を介して直列-並列変換回路2408に接続する赤外線モジュール301は、図 2 4 (b) に示すように、クレジット決済端末300とのインターフェイスであるシリアルポート2455と、直列-並列変換回路2408から入力するデジタル信号2458を、実際に、赤外線として送信するデジタル2460に変換し、または、受信したアナログ信号2461をシリアル・デジタル信号2459に復調する変換回路2458と、復調回路2458によって変調された信号2460を赤外線に変換して発光し、または、受光した赤外線をアナログ信号2461に変換する赤外線受光部2457とを具備している。

[0 3 3 1] この赤外線モジュール301は、赤外線通信の際に、赤外線を送信と受信とを行なう。赤外線モジュール301は、CPU 2400によって設定された送信データを赤外線に変換して送信し、また、受信した赤外線を受信データに変換する。

[0 3 3 2] また、キーボード制御部2411は、マーチャントがモジュール304、フックスイッチ305、ファンクションスイッチ306、テンキースイッチ307、実行スイッチ308または電源スイッチ309のいずれかを押すと、割り込み信号2439をアサする。この割り込み信号2439は、CPU 2400に、スイッチ操作に対応する処理を促す。また、キーボード制御部2411は、図 2 7 (a) に示すように、各スイッチの有効/無効を設定するキー操作制御レジスタ (KEYCTL) 2710を具備している。CPU 2400は、このキー操作制御レジスタ (KEYCTL) 2710をアクセスして、各スイッチの有効/無効を設定する。

[0 3 3 3] 音声処理部2413は、図 2 7 (a) に示すように、音声処理動作を制御する音声処理制御レジスタ (SCTL) 2709を具備している。CPU 2400は、この音声処理制御レジスタ (SCTL) 2709にアクセスして、音声処理部2413の動作を制御する。例えば、デジタル電話の着呼要求を受信した場合に、CPU 2400は、音声処理制御レジスタ (SCTL) 2709にアクセスして、デジタル電話の着呼信号を出力する設定を行なう。そうすることによって、音声処理部2413がスピーカ2412をドライブし、デジ

タル電話の着呼信号が出力される。

[0 3 3 4] また、音声コーデック2414は、音声処理部2413から入力するアナログ音声信号2444のデジタル音声データへの符号化と、チャネルコーデック2415から入力するデジタル音声データのデジタル音声信号2443への復号化とを行なう。アナログ音声信号2443は、音声処理部2413へ供給され、音声処理部2413が、アナログ音声信号2443を増幅し、受話器303のレシーバをドライブすることによって、レシーバから音声信号が出力される。一方、符号化によって生成されたデジタル音声データは、チャネルコーデック2415へ供給され、通信チャネルに乗る送信データに変換される。

[0 3 3 5] チャネルコーデック2415には、送信するデータとして、二種類のデータが入力される。一つは、音声コーデック2414から入力するデジタル音声データであり、もう一つは、CPUから、制御ロジック2410を介して、入力するデータ通信データである。

[0 3 3 6] チャネルコーデック2415は、デジタル音声データとデータ通信データとの識別情報と、ヘッダ情報として、それぞれのデータに付加して、デジタル音声データとデータ通信データとが多重化されたデジタル信号2448をデジタル通信アダプタ2416へ供給する。

[0 3 3 7] その逆に、チャネルコーデック2415は、デジタル通信アダプタ2416から入力するデジタル信号2448に対して、まず、ターミナルIDを照合し、次に、データのヘッダ情報から、デジタル音声データとデータ通信データとを識別し、それぞれ、音声コーデック2412と制御ロジック2410とへ供給する。また、チャネルコーデック2415は、デジタル電話を着信した時、及びデータ通信データを受信した時に、割り込み信号2449をアサする。割り込み信号2449は、CPU 2400に、デジタル電話の着信時の処理と、データ通信データの処理とを促す。

[0 3 3 8] チャネルコーデック2415は、こうした動作を行なうために、図 2 7 (a) に示すように、ターミナルIDを格納するIDレジスタ (ID) 2703と、チャネルコーデック2415の動作を制御するチャネルコーデック制御レジスタ (CCTL) 2704と、音声コーデック2414から入力されるデジタル音声データを格納する音声送信バッファ2705と、受信データの中から抽出したデータ通信データを格納するデータ受信バッファ2708とを具備している。

[0 3 3 9] デジタル通信アダプタ2416は、デジタル信号2448を、デジタル電話通信のフォーマットにエンコードしてデジタル電話通信回路110に出力する。逆に、デジタル通信アダプタ2416は、デジタル電話通信回路110から受信した信号をデコードして、デジタル信号2448から受信した信号をデコードして、デジタル信号2448



(41)

(42)

を、チャンネルコードが1415に接続する。  
[03040] R-S-232Cインターフェース1417は、  
R-S-232Cインターフェイス1313を接続するインターフェース  
回路であり、ケリジツ技術編集は、このR-S-232C  
インターフェース1417を介して、キヤッシュレジスタ  
311と通信する。R-S-232Cインターフェース1417  
は、キヤッシュレジスタ311からデータを受信すると、  
割り込み信号3455をアサトする。割り込み信号3455  
は、CPU2400に、R-S-232Cインターフェース1411  
を介した、キヤッシュレジスタ311とのデータ通信の処  
理を促す。

〔0341〕また、制御ロジック部2101は、図27  
(a)に示すように、その内部に、クロックカウンタ(C  
LOCK)2700、アップデータ時刻レジスタ(UPDATE)2701、  
及び組み込みレジスタ(INT)2702の3つのレジスタを内  
蔵する。

【0342】クロックカウンタは、現在の時刻をカウンタするカウンタ、フリップフロップ時刻レジスタは、クロックアップクロック100が、サード提供システムと通信して、RAM242及びハードディスク243上のデータを更新する処理（データレジスタ処理）を行なう時刻を格納するレジスタ、割り込みレジスタは、CPU340への割り込みの要因を示すレジスタである。

【0343】制御ロジック部3410は、割り込み番号233  
9,2449,2450のいずれかの割り込み番号がスタートされ  
ると、その割り込み要因を、割り込みレジスタ(1)N727C  
2に設定し、割り込み番号2418を「スタート」、CPU  
2に割り込み処理を促す。CPU2は、割り込み要因  
で、割り込みレジスタを読み出し、その割り込み要因に  
応じた処理を行なう。

【0344】 割り込みレジスタ(INT)の各ビットフィールドは、図27 (b) に示すように意味づけられている。

【0345】 ビット31は、電源スイッチの状態を示し、値が0の時、パワーオフの状態であることを示し、値が1の時、パワーオン状態であることを示す。

【0346】ビット30は、デジタル電話通信の状態を示し、値が0の時、デジタル電話通信をしていない状態であることを示し、値が1の時、デジタル電話通信をしている状態であることを示す。

【0347】ビット28は、増値料込の発生を示し、値が1の時、デジタル電話を増値したことを示す。このビットフィールドには、デジタル電話を増値し、割り込番号449がスタートされた時に、1が設定される。

【0348】ビット27は、データ受信側の発生を示し、値が1の時、データ受信データを受信したことを示す。このビットフィールドには、デジタル電話通信に基いて、データ通信データを受信し、割り込み信号2449を送信する時に、1が設定される。

促すアツプデート割込の発生を示し、値が1の時、アツプデート割込が起こったことを示す。このビットフィールドには、クロックカウンタの値がアツプデート時刻レジスタの値に一致した時に、1が設定される。

【0350】ビット25は、キヤジュアルスタビリティのデータ通信の処理を促す外部1F割込の発生を示し、値が1の時、外部1F割込が起こつたことを示す。このビット1以外のものは、RS-232Cインタフェース241から入力する割り込み番号246がアサートされた時に、1が設定される。

【0351】ビット24は、スイッチ操作によるキー番  
込の発生を示し、値が1の時、キー割込が起ったこと  
を示す。

103521 また、ビット0からビット11は、それぞれ、ビット10とビット11は、それぞれ、デジャースイッチの“\*”と“#”のスイッチに接続し、ビット12からビット15は、それぞれ、フランクショナルスイッチの“P1”から“P4”のスイッチに接続し、ビット16からビット18は、それぞれ、電源スイッチ、実行スイッチ、モードスイッチ、通話スイッチに接続し、ビット20は、フランクスイッチに接続し、ビットの値が1の時、そのビットに接続するスイッチが、押されたことを示す。

【03563】次に、RAM2402に格納されるデータに  
して説明する。  
【03564】図25は、RAM2402に格納されるデー  
タのRAMチップの模式図である。

[0365] R.AM3400は、基本プログラム領域R500、ユーエスデータ領域R501、マシントラップ領域R502、ワーク領域R503、及びプログラムの領域R504の五つの領域がある。基本プログラム領域R500は、ROM3401に格納されているプログラムのバージョンアップされたものが、メモリ、フラッシュメモリー等の記憶装置に格納されて、マシントラップ領域R502は、マシントラップが格納される領域、R.AM3503は、マシントラップが自由に使用できる領域、ワーク領域R504は、CPU0004、プログラムを実行する際に使用する作業領域、マシントラップ領域R504は、マシントラップの実行が受信した情報、一時的に、格納する領域である。

【0356】サービステータ領域501は、パーソナルリモート・クレジット状のサービスのID情報や、取クレジットカード情報、履歴情報を格納する領域であり、この領域のデータは、サービステータスデータによって管理される。

【03571】サービステータ領域3501には、さらに、  
ータ管理情報3503、マニフェスト設定情報3506、電話  
報3507、ケーブルジョイントリスタ3508、及び販売履歴  
スト3509の5つ領域がある。

【03581】データ管理情報3505は、サービステータ  
域3501に格納されている情報の管理情報を格納する領  
域3501に格納されている情報の管理情報を格納する領

域、サーチャント設定情報5016は、パーソナル・リモ  
ト・コントロール決断サービスに関する。サーチャントの  
設定情報を格納する領域、電話情報5017は、デジタリ  
域に関連する情報を格納する領域、コントロールドリ  
フト5018は、サーチャントが取り決めごとができるクレ  
ッドカードのリスト情報を格納する領域、販売履歴リ  
スト5019は、パーソナル・リモート・コントロール決断サ  
ービスでの販売の履歴情報を格納する領域である。  
10359) 次に、サーチャント領域501に格納され  
る情報について詳しく説明する。  
10360) 図26は、サーチャント領域501に格納  
される情報の関係を詳細に表した模式図である。

「サビエラ・リモン・クレジント・技術・サービス」の2つの資産は格納されている。クレジント・カード番号3610(3611, 3614)は、サービス・センターが取り扱うことができないクレジント・カードの名称を示し、サービス・コード・リスト・アイテム3611(3613, 2615)は、そのクレジント・カードによって提供されるサービスの内、サービス・センターが取り扱うことができないサービス・コードを示すサービス・コード・リストが格納されている。アイテム3614(3613)のアドレスを示す。

「03661」販売履歴・サービス2509は、パーソナル・リモン・クレジント・技術・サービスでの販売の履歴情報を格納する領域である。販売履歴・サービス2509では、一つのパーソナル・リモン・クレジント・技術・サービスでの販売に

【0361】データ管理情報2605は、ツラツデータ日時2600、次回ツラツデータ日時2601、ターミナル、ステイ2602、データシート設定情報アドレス2603、電話番号アドレス2604、クレジットカードリスト・アドレス2605及び販売履歴リスト・アドレス2606の7つの情報によって構成される。

に対して、トランプ・サジョン番号2616(2630)、サー・ヒスコ  
ト2617(2621)、販売時刻2618(2622)、販売情報アドレス  
2619(2623)の4つの情報値が格納される。

は、後で詳しく説明する。

【0368】販売情報アドレス3619(6633)には、ハードウェアアドレス3403上のアドレスを示すローカルアドレス、また、サブアドレス3404上のアドレスを示すリモートアドレス、また、アドレス3405上のアドレスを示すリモートアドレスが格納される。販売情報アドレス3619(6633)に、リモートアドレス3405は、決済完了通知が格納されているアドレスを示す。

【0363】ターミナル・ステータス2603は、クレジット決済端の状態を示し、サーチャント設定情報2604と2603、電話情報2605、クレジットカードリスト2606、電話2605、販売履歴リスト・アドレス2606は、それぞれ、サーチャント設定情報2606、電話情報2607、クレジットカードリスト2608、利用履歴リスト2609が格納されている領域の先頭番地を示す。

[0369] 販売情報アドレス1619(323)に格納される  
アドレスは、サービスタップシステムによって決定され  
る。データリタッチャー（処理の順に、各販売情報の販売

07. 電話番号が「トリス3608」、短縮ダイヤル設定が「トリス16090」3つの情報によって構成される。発信元電話番号6071の情報は、この情報は、デジタル無線電話の共通規格に用いられる。電話番号「トリス2608」と、短縮ダイヤル番号「トリス16090」と、それぞれ、電話番号情報、短縮ダイヤル設定が「トリス」が格納されている。デジタル403上の「トリス」を示す。

明示する。  
 [0371] 図28は、CPU3400が行なう処理のフロー概略図である。  
 [0372] 図28に示すように、CPUの処理は、大

【0365】クレジットカードリスと500には、マーズヤントが取り扱うことができるクレジットカードのリスと250ト情報格納されている。クレジットカードリスと250では、一つのクレジットカードに対して、クレジットカード名各2610(2612, 2610)、サービスコード・リスと、ア

大きく分けて、10種類のフロセスと、新造処理2601とに分けることが出来る。  
 (0373) 10種類のフロセスとは、パワーオンフロセス、電話フロセス、クレンジット決着フロセス、顧客サービスコールフロセス、問い合わせコールフロセス、デ

(43)

ータアップデートプロセス、リモートアクセスプロセス、セッション確立プロセス、外部 I/F 通信プロセス、及びパワーオンプロセスであり、この 10 種類のプロセスは、メインルーブル2800の中で実行される。各プロセスには、そのプロセスに対応して、プロセスのステータス(状態)を示すワーディングフィールドが RAM402上に存在し、CPU400は、このプロセスステータスの値に応じて、各プロセスを実行する。

[0 3 7 4] パワーオンプロセスは、マーチャントが電源スイッチをオンした時の初期動作処理を行なうプロセス、電話プロセスは、デジタル電話モード時の処理を行なうプロセス、クレジット決済プロセスは、クレジット決済モード時の処理を行なうプロセス、顧客サービスコールプロセスは、“顧客サービスコール”の処理を行なうプロセス、問い合わせコールプロセスは、“問い合わせコール”の処理を行なうプロセス、データアップデートプロセスは、データアップデート処理を行なうプロセス、リモートアクセスプロセスは、サービス提供システムのマーチャント情報サーバ上のデータをアクセスする処理を行なうプロセス、セッション確立プロセスは、サービス提供システムとの通信セッションを確立する処理を行なうプロセス、外部 I/F 通信プロセスは、キャッシュレジスタ11とのデータ通信を行なうプロセス、パワーオンプロセスは、マーチャントが電源スイッチをオフした時の終了処理を行なうプロセスである。

[0 3 7 5] 図 28 において、クレジット決済端末をリセットすると、ステップ2802へ進み、CPU400は、パワーオンプロセスを“active”にする。次に、ステップ2803で、パワーオンプロセスが“active”か否かを調べ、“inactive”の場合、ステップ2805へ進み、“active”の場合は、ステップ2804へ進み、パワーオンプロセスを一定時間実行して、ステップ2805へ進む。

[0 3 7 6] ステップ2805では、電話プロセスが“active”か否かを調べ、“inactive”の場合は、ステップ2807へ進み、“active”の場合は、ステップ2806へ進み、電話プロセスを一定時間実行して、ステップ2807へ進む。

[0 3 7 7] ステップ2807では、クレジット決済プロセスが“active”か否かを調べ、“inactive”の場合は、ステップ2809へ進み、“active”の場合は、ステップ2808へ進み、クレジット決済プロセスを一定時間実行して、ステップ2809へ進む。

[0 3 7 8] ステップ2809では、顧客サービスコールプロセスが“active”か否かを調べ、“inactive”の場合は、ステップ2810へ進み、顧客サービスコールプロセスを一定時間実行して、ステップ2811へ進む。

[0 3 7 9] ステップ2811では、問い合わせコールプロセスが“active”か否かを調べ、“inactive”の場合は、ステップ2813へ進み、“active”の場合は、ステッ

プ2812へ進み、問い合わせコールプロセスを一定時間実行して、ステップ2813へ進む。ステップ2813では、データアップデートプロセスが“active”か否かを調べ、“inactive”の場合は、ステップ2815へ進み、“active”の場合は、ステップ2814へ進み、データアップデートプロセスを一定時間実行して、ステップ2815へ進む。

[0 3 8 0] ステップ2815では、リモートアクセスプロセスが“active”か否かを調べ、“inactive”の場合は、ステップ2817へ進み、“active”の場合は、ステップ2816へ進み、リモートアクセスプロセスを一定時間実行して、ステップ2817へ進む。セッション確立プロセスが“active”か否かを調べ、“inactive”の場合は、ステップ2819へ進み、“active”の場合は、ステップ2818へ進み、セッション確立プロセスを一定時間実行して、ステップ2819へ進む。

[0 3 8 1] ステップ2819では、外部 I/F 通信プロセスが“active”か否かを調べ、“inactive”の場合は、ステップ2821へ進み、“active”の場合は、ステップ2820へ進み、外部 I/F 通信プロセスを一定時間実行して、ステップ2821へ進む。

[0 3 8 2] ステップ2821では、パワーオンプロセスが“active”か否かを調べ、“active”の場合、ステップ2822へ進み、パワーオンプロセスを実行し、“inactive”の場合は、ステップ2823へ戻る。

[0 3 8 3] また、CPU400は、割り込み番号418がアサートされると、割込処理2801を実行し、元のメインルーブル2800の処理に戻る。

[0 3 8 4] 割込処理2801では、まず、CPU400は、ステップ2823で、割り込みレジスタ(IN7)2705を読みだし、RAM1502のワーク領域3503上のワードInterruptにコピーする。この時、CPU400に読み出された割り込みレジスタ(IN7)2705は、エコーリセットされる。

[0 3 8 5] 次に、ステップ2824で、Interruptのビット28の値から、着信割込か否かを調べ、着信割込でない場合(Interrupt(b1128)=0)、ステップ2825へ進み、電話プロセスのプロセスステータスを“active”にして、ステップ2826へ進む。

[0 3 8 6] ステップ2826では、Interruptのビット26の値から、アップデート割込か否かを調べ、アップデート割込でない場合(Interrupt(b1126)=0)、ステップ2828へ進み、アップデート割込の場合(Interrupt(b1126)=1)、ステップ2827へ進み、データアップデートプロセスのプロセスステータスを“active”にして、ステップ2828へ進む。

[0 3 8 7] ステップ2828では、Interruptのビット25の値から、外部 I/F 割込か否かを調べ、外部 I/F 割込でない場合(Interrupt(b1125)=0)、ステップ2830へ進み、外部 I/F 割込の場合(Interrupt(b1125)=1)、ステップ2829へ進み、外部 I/F 通信プロセスのプロセスステ

(44)

ィタスを“active”にして、ステップ2830へ進む。

[0 3 8 8] ステップ2830では、Interruptのビット24の値から、キー割込か否かを調べ、キー割込でない場合(Interrupt(b1124)=0)、割込処理を終了し、元のメインルーブルの処理へ戻り、キー割込の場合(Interrupt(b1124)=1)は、ステップ2831へ進む。

[0 3 8 9] ステップ2831では、Interruptの“電源”ビット(b1116)の値を調べ、0の場合は、割込処理を終了し、元のメインルーブルの処理へ戻り、1の場合は、電源スイッチが操作されたと判定し、ステップ2832へ進む。

[0 3 9 0] ステップ2832では、Interruptの“パワー表示”ビット(b1131)の値を調べ、0の場合には、パワーオンの操作が行なわれたと判定し、ステップ2834へ進み、1の場合には、パワーオンの操作が行なわれたと判定し、ステップ2833へ進む。

[0 3 9 1] ステップ2833では、パワーオンプロセスのプロセスステータスを“active”にして、割込処理を終了し、元のメインルーブルの処理へ戻る。

[0 3 9 2] ステップ2834では、パワーオンプロセスのプロセスステータスを“active”にして、割込処理を終了し、元のメインルーブルの処理へ戻る。

[0 3 9 3] 割込処理2801の中で、プロセスステータスが“active”になったプロセスは、メインルーブルに戻り、メインルーブルの中で実行される。

[0 3 9 4] 次に、サービス提供システム102のユーザ情報サーバ402に格納される情報について説明する。

[0 3 9 5] 図 29 は、一人のユーザに対して、ユーザ情報サーバ402に格納される情報を表した模式図である。

[0 3 9 6] ユーザ情報サーバ402では、一人のユーザに対して、ユーザデータ管理情報2900、個人情報2901、写真データ2902、ターミナル・プロパティ2903、ユーザ設定情報2904、アクセス制御情報2905、端末データ2906、電話情報2907、クレジットカード・リスト2908、及び利用履歴リスト2909の10種類の情報が格納される。ユーザデータ管理情報2900は、一人のユーザに関して、ユーザ情報サーバ402に格納される情報の管理情報である。

[0 3 9 7] 個人情報2901は、ユーザの年齢、生年月日、職業、口座番号、契約内容等の個人に関する情報であり、この情報の一部が、パーソナル・クレジット端末100の個人情報606に対応している。

[0 3 9 8] 写真データ2902は、ユーザの顔写真のデータ、ターミナル・プロパティ2903は、パーソナル・クレジット端末100の型番、シリアル番号、RAM容量、格納されているプログラムのバージョン等のパーソナル・クレジット端末100の属性情報である。

[0 3 9 9] ユーザ設定情報2904は、パーソナル・リモート・クレジット決済サービスに関する、ユーザの設定

情報であり、パーソナル・クレジット端末100のユーザ設定情報608に対応する情報である。

[0 4 0 0] アクセス制御情報2905は、顧客サービスコールにおけるアクセス制御に関するユーザの設定情報、端末データ2906は、パーソナル・クレジット端末100のRAMデータ、電話情報2907は、デジタル無線電話に連する情報であり、パーソナル・クレジット端末100の電話情報609に対応する情報である。

[0 4 0 1] クレジットカード・リスト2908は、ユーザが登録したクレジットカードのリスト情報、利用履歴リスト2909は、パーソナル・リモート・クレジット決済サービスの利用履歴情報である。

[0 4 0 2] ユーザデータ管理情報2900は、ユーザ名2910、ユーザ ID2911、ユーザ・ステータス2912、個人情報2913、写真データアドレス2914、ユーザ公開鍵2915、ターミナル・プロパティ・アドレス2916、ユーザ設定情報アドレス2917、アクセス制御情報アドレス2918、アップデート日時2919、次回アップデート日時2920、端末データアドレス2921、電話情報アドレス2922、クレジットカード・リスト・アドレス2923、及び利用履歴リスト・アドレス2924の15個の情報によって構成される。

[0 4 0 3] ユーザ・ステータス2912は、パーソナル・クレジット端末100の状態を示し、パーソナル・クレジット端末100のターミナル・ステータス1702に対応する情報である。

[0 4 0 4] アップデート日時2919は、前回、パーソナル・クレジット端末100のサービスデータ領域1601のデータを更新した日時を示し、次回アップデート日時2920は、次のサービスデータ領域1601のデータの更新の予定日時を示し、それぞれパーソナル・クレジット端末100のアップデート日時1700と次回アップデート日時1701とに対応する。

[0 4 0 5] 個人情報アドレス2913、写真データアドレス2914、ターミナル・プロパティ・アドレス2916、ユーザ設定情報アドレス2917、アクセス制御情報アドレス2918、端末データアドレス2921、電話情報アドレス2922、クレジットカード・リスト・アドレス2923、及び利用履歴リスト・アドレス2924は、それぞれ、個人情報2901、写真データ2902、ターミナル・プロパティ2903、ユーザ設定情報2904、アクセス制御情報2905、端末データ2906、電話情報2907、クレジットカード・リスト2908、及び利用履歴リスト2909が格納されているユーザ情報サーバ402上のアドレスを示す。

[0 4 0 6] 端末データ2906は、前回、アップデート処理した際のパーソナル・クレジット端末100のRAM1502上のデータであり、次のアップデート処理の際のデータと比較、及び、バックアップデータとして用いられる。

[0 4 0 7] クレジットカード・リスト2908及び利用履歴

(45)

リスト33008。それぞれ、パーソナル・クレジット端末1000クレジットカードリスト1610と利用履歴リスト1611に対応する情報である。但し、イミナル・データ・アドレス3944、オプティカル・データ・アドレス3945、及び利用履歴アドレス3954は、すべて、ユーザ情報サーバ403上のアドレスを示す。

[0 4 0 8] 次に、ユーザ提供システム103のユーザメント情報サーバ403に格納される情報について説明する。

[0 4 0 9] 図3 0は、一つのユーザメントに対して、ユーザメント情報サーバ403で、ユーザメント情報サーバ403に格納される情報を変えた図式図である。

[0 4 1 0] ユーザメント情報サーバ403では、一つのユーザメントに対して、ユーザメントデータ管理情報3000、ユーザメント情報3001、ターミナル・プロバイダ3002、ユーザメント設定情報3003、端末データ3004、電話情報3005、クレジットカード・リスト3006、及び販売履歴リスト3007の8種類の情報が格納される。

[0 4 1 1] ユーザメントデータ管理情報3000は、一つのユーザメントに関して、ユーザメント情報サーバ403に格納される情報の管理情報である。

[0 4 1 2] ユーザメント情報3001は、ユーザメントの住所、口番番号、契約内容等のユーザメントに関する情報であり、ターミナル・プロバイダ3002は、クレジット端末3000の型番、シリアル番号、RAM容量、ハードディスク容量、格納されているプログラムのバージョン等のクレジット端末3000の属性情報である。

[0 4 1 3] ユーザメント設定情報3003は、パーソナル・リモート・クレジット端末サービスに関する、ユーザメントの設定情報であり、クレジット端末3000のユーザメント設定情報3004に対応する情報である。

[0 4 1 4] 端末データ3004は、クレジット端末3000のRAM102と、ハードディスク303のデータ、電話情報3005は、デジタル電話に関連する情報であり、クレジット端末3000の電話情報3007に対応する情報である。

[0 4 1 5] クレジットカードリスト3008は、ユーザメントが取り扱うことができるクレジットカードのリスト情報、販売履歴リスト3007は、パーソナル・リモート・クレジット端末サービスでの販売履歴情報である。

[0 4 1 6] ユーザメントデータ管理情報3000は、ユーザメント名3006、ユーザメントID3009、ユーザメント・ステータス3010、ユーザメント情報アドレス3011、ユーザメント公開鍵3012、ターミナル・プロバイダ・アドレス3013、ユーザメント設定情報アドレス3014、アップロード日時3015、次回アップロード日時3016、端末データアドレス3017、電話情報アドレス3018、クレジットカード・リスト・アドレス3019、及び販売履歴リスト・アドレス3020の13個の情報によって構成される。

[0 4 1 7] ユーザメント・ステータス3010は、クレジット端末3000の状態を示し、クレジット端末3000のターミナル・ステータス1602に対応する情報である。

[0 4 1 8] アップロード日時3015は、前回、クレジット端末3000のユーザメント領域1603のデータを更新した日時を示し、次回アップロード日時3016は、次のユーザメント領域1603のデータの更新の予定日時を示し、クレジット端末3000のアップロード日時3600と次回アップロード日時3601とに対応する。

[0 4 1 9] ユーザメント情報アドレス3011、ターミナル・プロバイダ・アドレス3013、ユーザメント設定情報アドレス3014、端末データアドレス3017、電話情報アドレス3018、クレジットカード・リスト・アドレス3019、及び販売履歴リスト・アドレス3020は、それぞれ、ユーザメント情報3001、ターミナル・プロバイダ3002、ユーザメント設定情報3003、端末データ3004、電話情報3005、クレジットカード・リスト3006、及び販売履歴リスト3007が格納されているユーザメント情報サーバ403上のアドレスを示す。

[0 4 2 0] 端末データ3004は、前回、アップロード処理した際のクレジット端末3000のRAM3402と、ハードディスク303とのデータであり、今回のアップロード処理の際のデータ比較、及び、バックアップデータとして用いられる。

[0 4 2 1] クレジットカードリスト3008及び販売履歴リスト3007も、それぞれ、クレジット端末3000のクレジットカードリスト3508と販売履歴リスト3509とに対応する情報である。但し、販売履歴アドレス3043は、すべて、ユーザメント情報サーバ403上のアドレスを示す。

[0 4 2 2] 次に、ユーザ提供システム103の決済処理履歴情報サーバ404に格納される情報について説明する。

[0 4 2 3] 図3 1は、一つの決済処理履歴に対して、決済処理履歴情報サーバ404に格納される情報を変えた図式図である。

[0 4 2 4] 決済処理履歴情報サーバ404では、一つの決済処理履歴に対して、決済処理履歴データ管理情報3100、決済処理履歴情報3101、クレジットカード・リスト3102、及び販売履歴リスト3103の4種類の情報が格納される。

[0 4 2 5] 決済処理履歴データ管理情報3100は、一つの決済処理履歴に関して、決済処理履歴情報サーバ404に格納される情報の管理情報である。決済処理履歴情報3101は、決済処理履歴の住所、口番番号、契約内容等の決済処理履歴に関する情報であり、クレジットカード・リスト3102は、決済処理履歴が取り扱うことができるクレジットカードのリスト情報、決済履歴リスト3103は、パーソナル・リモート・クレジット端末サービスでの決済履歴情報である。

[0 4 2 6] 決済処理履歴データ管理情報3100は、決済

(46)

処理履歴名3104、決済処理履歴ID3105、決済処理履歴ステータス3106、決済処理履歴情報アドレス3107、決済処理履歴公開鍵3108、クレジットカード・リスト・アドレス3109、及び決済履歴リスト・アドレス3110の7個の情報によって構成される。

[0 4 2 7] 決済処理履歴ステータス3106は、決済システム103の決済処理のサービス状態を示し、決済処理履歴情報アドレス3107、クレジットカード・リスト・アドレス3109、決済履歴リスト・アドレス3110は、それぞれ、決済処理履歴情報3101、クレジットカード・リスト3102、決済履歴リスト3103が格納されている決済処理履歴情報サーバ404上のアドレスを示す。

[0 4 2 8] クレジットカードリスト3102には、決済処理履歴が取り扱うことができるクレジットカードのリスト情報を示す。クレジットカードリスト3107では、一つのクレジットカードに対して、クレジットカード名3111(3115)、サブ・アドレスコード・リスト・アドレス3112(3113、3116)、サブ・アドレスコード・リスト・アドレス3112(3114、3116)の2つの情報が格納されている。

[0 4 2 9] クレジットカード名3111(3113、3116)は、決済処理履歴が取り扱うことができるクレジットカードの名前を示し、サブ・アドレスコード・リスト・アドレス3112(3114、3116)は、そのクレジットカードによって提供されるサブ・アドレスの内、決済処理履歴が取り扱うことができるサブ・アドレスの履歴を示すサブ・アドレスが格納されている決済処理履歴情報サーバ404上のアドレスを示す。

[0 4 3 0] 決済履歴リスト3103は、パーソナル・リモート・クレジット決済サービスでの決済の履歴情報を格納する領域である。

[0 4 3 1] 決済履歴リスト3103では、一つのパーソナル・リモート・クレジット決済サービスでの決済に対して、決済番号3119(3123)、決済情報アドレス3120(3124)の4つの情報が格納される。

[0 4 3 2] 決済番号3119(3123)は、決済処理をユニークに示す決済完了通知620を生成する際に決済システムが発行する番号、サブ・アドレスコードの種別を示すコード番号、決済時刻3119(3123)は、パーソナル・リモート・クレジット決済サービスで決済した時刻、決済情報アドレス3120(3124)は、決済システム103が発行した決済完了通知が格納されている決済処理履歴情報サーバ404上のアドレスを示す。

[0 4 3 3] 次に、ユーザ提供システム103のサブ・アドレス3124に格納される情報を変えた図式図である。

[0 4 3 4] 図3 2は、サブ・アドレス3124情報サーバ404に格納される情報を変えた図式図である。

[0 4 3 5] サブ・アドレス3124情報サーバ404には、ユーザリスト3200、ユーザメントリスト3201、決済処理履歴リスト3202、サブ・アドレス提供履歴リスト3203、及び決済処理履歴データ管理情報3204の5種類の情報が格納される。

[0 4 3 6] ユーザリスト3200は、サブ・アドレス提供者と契約をしている全ユーザの属性情報のリスト、ユーザメントリスト3201は、サブ・アドレス提供者と契約をしている全ユーザメントの属性情報のリスト、決済処理履歴リスト3202は、サブ・アドレス提供者と契約をしている全決済処理履歴の属性情報のリスト、サブ・アドレス提供履歴リスト3203は、パーソナル・リモート・クレジット決済サービスでの提供したサブ・アドレスの履歴情報のリストであり、決済処理履歴データ管理情報3204は、ユーザ及びユーザメントからのパーソナル・リモート・クレジット決済サービスの要求に対して、関連な決済処理履歴を対応付けたデータ管理情報である。

[0 4 3 7] ユーザリスト3200には、一人のユーザに対して、ユーザ名3205(3209)、ユーザID3206(3210)、ユーザ電話番号3207(3211)、サブ・アドレス・リスト・アドレス3208(3212)の4種類の情報が格納されている。

[0 4 3 8] サブ・アドレス・リスト・アドレス3208(3212)は、ユーザが利用できるサブ・アドレスコードのリストが格納されているサブ・アドレスデータ管理情報サーバ404上のアドレスを示す。

[0 4 3 9] ユーザメントリスト3201には、一つのユーザメントに対して、ユーザメント名3213(3218)、ユーザメントID3214(3219)、ユーザメント電話番号3215(3220)、サブ・アドレス・リスト・アドレス3216(3221)、顧客データ・アドレス3217(3222)の5種類の情報が格納されている。

[0 4 4 0] サブ・アドレス・リスト・アドレス3216(3221)は、ユーザメントが取り扱うことができるサブ・アドレスコードのリストが格納されているサブ・アドレスデータ管理情報サーバ404上のアドレスを示す。

[0 4 4 1] 顧客データ・アドレス3217(3222)は、顧客番号とユーザIDとに対応を示すデータ管理情報が格納されているサブ・アドレスデータ管理情報サーバ404上のアドレスを示す。

[0 4 4 2] 決済処理履歴リスト3202には、一つの決済処理履歴に対して、決済処理履歴名3223(3227)、決済処理履歴ID3224(3228)、決済処理履歴住所ID3225(3229)、サブ・アドレス・リスト・アドレス3226(3230)の4種類の情報が格納されている。

[0 4 4 3] 決済処理履歴住所ID3225(3229)は、サブ・アドレス提供システム103が、デジタル通信回線111を介して決済システム103と通信する際の決済システム103のIDを示し、サブ・アドレス・リスト・アドレス3226(3230)は、決済処理履歴が取り扱うことができるサブ・アドレスコードのリストが格納されているサブ・アドレスデータ管理情報サーバ404上のアドレスを示す。

[0 4 4 4] サブ・アドレス提供履歴リスト3203には、パーソナル・リモート・クレジット決済サービスのサブ・

(47)

ビス提供に対して、サービス提供番号3231(3235)、サービスコード3232(3236)、サービス提供時刻3233(3237)、サービス提供情報アドレス3234(3238)の4つの情報が格納されている。

[0 4 4 5] サービス提供番号3231(3235)は、一つのサービス提供におけるサービス提供システム102での処理をユニークに示す番号、サービスコード3232(3236)は、ユーザが利用したクレジットカードサービスの種類を示すコード番号、サービス提供時刻3233(3237)は、パーソナル・リモートクレジットカードのサービスのサービスを提供した時刻、サービス提供情報アドレス3234(3238)は、一つのサービス提供におけるサービス提供システム102での処理の履歴情報が格納されているサービスディレクトリ情報サバーバ101上のアドレスを示す。

[0 4 4 6] 次に、パーソナル・クレジットカード100、または、クレジットカード300において、リモートアドレスにあるデータをアクセスした場合に行なうダウンロードの処理について説明する。以下では、この処理を、リモートアクセス処理と呼ぶこととする。

[0 4 4 7] 図3 3 (a) は、リモートアクセス処理の手順を示し、図3 4 (a)、(b) は、交換するメッセージの内容を示している。アクセスしたデータが、リモートアドレスにあった場合、パーソナル・クレジットカード100(クレジットカード300)は、サービス提供システム102にデータを要求するメッセージ、リモートアクセス要求3300を生成し、サービス提供システム102に送信する。

[0 4 4 8] 図3 4 (a) に示すように、リモートアクセス要求3300は、メッセージがリモートアクセス要求3300であることを示すヘッダ情報、リモートアクセス要求ヘッダ3400と、リモートアドレスを示すデータアドレス3401と、ユーザID(マーチャントID) 3402と、このリモートアクセス要求3300を発行した日時を示す発行日時3403とから成るデータについて、ユーザ(マーチャント)のデジタル署名3404を行ない、サービス提供者宛に封書化したものである。

[0 4 4 9] サービス提供システム102は、リモートアクセス要求3300を受信し、暗号を復号化し、デジタル署名をチェックして、要求されたデータをパーソナル・クレジットカード100(クレジットカード300)に送るメッセージ、リモートアクセスデータ3301を生成し、パーソナル・クレジットカード100(クレジットカード300)に送る。

[0 4 5 0] 図3 4 (b) に示すように、リモートアクセスデータ3301は、メッセージがリモートアクセスデータ3301であることを示すヘッダ情報、リモートアクセスデータヘッダ3400と、要求されたデータ3403と、サービス提供者1 D 3410と、このリモートアクセスデータ3301を発行した日時を示す発行日時3411とから成るデータについて、サービス提供者のデジタル署名を行ない、ユー

ザ(マーチャント)宛に封書化したものである。

[0 4 5 1] パーソナル・クレジットカード100(クレジットカード300)は、リモートアクセスデータ3301を受信し、暗号を復号化し、デジタル署名をチェックして、テンポラリ領域に格納して、データにアクセスする。

[0 4 5 2] 次に、パーソナル・クレジットカード100及びクレジットカード300が、データアップデートプロセスにおいて行なうデータアップデート処理について説明する。

[0 4 5 3] 図3 3 (b) は、データアップデート処理の手順を示し、図3 4 (c) ~ (f) と図3 5 (a) は、交換するメッセージの内容を示している。

[0 4 5 4] パーソナル・クレジットカード100(クレジットカード300)は、データアップデートプロセスで、まず、サービス提供システム102に対して、データアップデート処理を要求するメッセージ、データアップデート要求3302を生成し、送信する。

[0 4 5 5] 図3 4 (c) に示すように、データアップデート要求3302は、メッセージがデータアップデート要求3302であることを示すヘッダ情報、データアップデート要求ヘッダ3416と、ユーザID(マーチャントID) 3417と、このデータアップデート要求3302を発行した日時を示す発行日時3418とから成るデータについて、ユーザ(マーチャント)のデジタル署名を行ない、サービス提供者宛に封書化したものである。

[0 4 5 6] サービス提供システム102は、データアップデート要求3302を受信し、暗号を復号化し、デジタル署名をチェックして、要求に対する暗号が出てくることを示すメッセージ、データアップデート要求3303を生成し、パーソナル・クレジットカード100(クレジットカード300)に送信する。

[0 4 5 7] 図3 4 (d) に示すように、データアップデート要求3303は、メッセージがデータアップデート要求3303であることを示すヘッダ情報、データアップデート要求ヘッダ3423と、サービス提供者1 D 3424と、このデータアップデート要求3303を発行した日時を示す発行日時3425とから成るデータについて、サービス提供者のデジタル署名を行ない、ユーザ(マーチャント)宛に封書化したものである。

[0 4 5 8] パーソナル・クレジットカード100(クレジットカード300)は、データアップデート要求3303を受信し、暗号を復号化し、デジタル署名をチェックし、RAM1502(クレジットカード300の場合は、RAM2403とハードディスク2403)のデータをサービス提供システム102にアップロードするメッセージ、アップロードデータ3304を生成し、サービス提供システム102に送る。

[0 4 5 9] 図3 4 (e) に示すように、アップロードデータ3304は、メッセージがアップロードデータ3304で

(48)

あることを示すヘッダ情報、アップロードデータヘッダ3430と、RAM1501(クレジットカード300の場合は、RAM2402とハードディスク2403)のデータを圧縮したデータ、端末データ3431と、ユーザID(マーチャントID) 3432と、このアップロードデータ3304を発行した日時を示す発行日時3433とから成るデータについて、ユーザ(マーチャント)のデジタル署名を行ない、サービス提供者宛に封書化したものである。

[0 4 6 0] サービス提供システム102は、アップロードデータ3304を受信し、暗号を復号化し、デジタル署名をチェックする。そして、圧縮された端末データ3431を解凍し、ユーザ情報サバーバ102(マーチャント情報サバーバ103)上の端末データ2908(端末データ3004)と照合する。

[0 4 6 1] そして、新しい端末データ2908(端末データ3004)を生成し、パーソナル・クレジットカード100(クレジットカード300)のデータをアップデートするメッセージ、アップデートデータ3305を生成して、パーソナル・クレジットカード100(クレジットカード300)に送信する。

[0 4 6 2] 図3 4 (f) に示すように、アップデートデータ3305は、メッセージがアップデートデータ3305であることを示すヘッダ情報、アップデートデータヘッダ3438と、新しい端末データを圧縮したデータ、端末データ3439と、サービス提供者1 D 3440と、このアップデートデータ3305を発行した日時を示す発行日時3441とから成るデータについて、サービス提供者のデジタル署名を行ない、ユーザ(マーチャント)宛に封書化したものである。

[0 4 6 3] パーソナル・クレジットカード100(クレジットカード300)は、アップデートデータ3305を受信し、暗号を復号化し、デジタル署名をチェックし、圧縮された端末データ3439を解凍して、RAM1502(クレジットカード300の場合は、RAM2402とハードディスク2403)のデータを更新する。

[0 4 6 4] サービス提供システム102は、新しい端末データの生成において、パーソナル・クレジットカード100に対しては、実体データ領域1612の容量に余裕が無い場合、各クレジットカードのアクセス時刻を比較し、アクセス時刻が最近のクレジットカードのオブジェクト・データ・アドレスにローカルアドレスを割り当て、各利用情報の利用時刻を比較し、利用時刻が最近の利用情報の利用時刻アドレスにローカルアドレスを割り当て、また、クレジットカード300に対しては、ハードディスク2403の容量に余裕が無い場合、各販売情報の利用時刻を比較し、利用時刻が最近の販売情報の販売情報アドレスにローカルアドレスを割り当てる。

[0 4 6 5] また、サービス提供システム102は、アップロードデータと端末データとを照合した際に、データの不正な改ざんが発見された場合には、アップデートデ

ータ3305の代わりに、パーソナル・クレジットカード100(クレジットカード300)の機能を停止させるメッセージ、機能停止命令3305を生成し、パーソナル・クレジットカード100(クレジットカード300)に送信する。[0 4 6 6] 図3 5 (a) に示すように、機能停止命令3305は、メッセージが機能停止命令3305であることを示すヘッダ情報、機能停止命令ヘッダ3500と、サービス提供者1 D 3501と、この機能停止命令3305を発行した日時を示す発行日時3502とから成るデータについて、サービス提供者のデジタル署名を行ない、ユーザ(マーチャント)宛に封書化したものである。

[0 4 6 7] この場合、機能停止命令3305を受信したパーソナル・クレジットカード100(クレジットカード300)は、暗号を復号化し、デジタル署名をチェックし、ターミナル・ステータス1702(ターミナル・ステータス2503)を“使用不能”に変更して、使用不能状態になる。

[0 4 6 8] また、パーソナル・クレジットカード100が、バックアッププロセスにおいて行なうバックアップ処理は、データアップデート処理と同じ手順で行なわれる。但し、アップデートデータ3305を受信して、RAM1503のデータを更新した後、ターミナル・ステータス1702を“書き込み不可”に変更して、バッテリリチの容量が十分状態になるまで、RAMへの新たなデータの入力を禁止する。

[0 4 6 9] 次に、“決済”の処理において、秘密鍵で交換されるデータの内容の詳細について説明する。[0 4 7 0] 図3 6 (a) ~ (f)、図3 7 (a) ~ (c)、図3 8 (a)、(b) は、“決済”の処理において、交換するメッセージの内容を示している。

[0 4 7 1] まず、ユーザが支払操作607をすると、パーソナル・クレジットカード100は、支払オフア608を生成し、赤外線通信で、クレジットカード300に送信する。

[0 4 7 2] 図3 6 (a) に示すように、支払オフア608は、メッセージが支払オフア608であることを示すヘッダ情報、支払オフアヘッダ3600と、サービスコード3601と、サービス提供者1 D 3602と、マーチャントの取引をユニークに示す番号として任意に生成した要求番号3603と、ユーザが入力した支払金額3604と、ユーザが入力した支払オプションを示す支払オプションコード3605と、この支払オフア608の有効期限3606と、この支払オフア608を発行した日時を示す発行日時3607とから成るデータについて、ユーザのデジタル署名を行なったものである。クレジットカード300は、支払オフア608を受信し、支払金額3604と請求金額とを照合し、支払オプション3605が利用可能なオプションであるか否かを照合して、支払オフア608を赤外線通信でパーソナル・クレジットカード100に送信し、信用照会要求410を生成して、デジタル電話通信でサービス提供

(49)

システム1031に送信する。

〔0473〕図36 (b) に示すように、支払オフナーは、メッセージが支払オフナーへ送客609であることを示すヘッダ情報、支払オフナーへ送客ヘッダ3608と、パーソナル・クレジット端末100が支払オフナーへ送客609を受信した際にLCD303に表示される送客メッセージ3609と、ユーザの取引をユニークに示す番号として任意に生成したトランザクション番号3610と、請求金額3611と、この支払オフナーの有効期限3612と、ヤーチャントID3613と、この支払オフナーへ送客609を発行した日時を示す発行日時3614とから成るデータについて、ヤーチャントのデジタル署名を行なったものである。送客メッセージ3609は、ヤーチャントのオフショーンで設定するテキストメッセージであり、設定されない場合もある。

〔0474〕図36 (c) に示すように、信用照会要求610は、メッセージが信用照会要求610であることを示すヘッダ情報、信用照会要求ヘッダ3615と、支払オフナー608と、支払オフナーへ送客609と、担当者名3616と、ヤーチャントID3617と、この信用照会要求610を発行した日時を示す発行日時3618とから成るデータについて、ヤーチャントのデジタル署名を行ない、サービス提供者宛に封鎖化したものである。担当者名3616は、ヤーチャントのオフショーンで設定する情報であり、設定されない場合もある。

〔0475〕パーソナル・クレジット端末100は、支払オフナーへ送客609を受信し、支払金額3404と請求金額とを照合して、支払要求613を生成し、デジタル無線電話通信で、サービス提供システム1031に送信する。

〔0476〕図36 (d) に示すように、支払要求613は、メッセージが支払要求613であることを示すヘッダ情報、支払要求ヘッダ3623と、支払オフナー608と、支払オフナーへ送客609と、ユーザID3624と、この支払要求613を発行した日時を示す発行日時3625とから成るデータについて、ユーザのデジタル署名を行ない、サービス提供者宛に封鎖化したものである。

〔0477〕サービス提供システム1031は、信用照会要求610と支払要求613を受信し、それぞれ、暗号を復号化し、デジタル署名をチェクする。そして、要求番号とトランザクション番号とヤーチャントIDとを照合して、取引をしようとしているヤーチャントとユーザとが、それぞれ、発行した信用照会要求610と支払要求613との対応となり、さらに、信用照会要求610と支払要求613との内容と照合して、信用照会送客614を生成し、デジタル無線通信で、クレジット決済端末3001に送信する。

〔0478〕図36 (e) に示すように、信用照会送客614は、メッセージが信用照会送客614であることを示すヘッダ情報、信用照会送客ヘッダ3630と、トランザクション番号3631と、信用照会の処理をユニークに示す番号

として任意に生成した照会番号3632と、信用照会の結果を示す照会結果3633と、ユーザの照の号、ユーザ3634

と、この信用照会送客614の有効期限を示す有効期限3635と、サービス提供者ID3636と、この信用照会送客614を発行した日時を示す発行日時3637とから成るデータについて、サービス提供者のデジタル署名を行ない、ヤーチャント宛に封鎖化したものである。信用照会の結果、ユーザの信用状況に問題がある場合は、写真データ3638は、設定されない。

〔0479〕クレジット決済端末3001は、信用照会送客614を受信し、暗号を復号化し、デジタル署名をチェクして、信用照会の結果をLCD302に表示する。

〔0480〕次に、ヤーチャントの担当者が、決済処理要求メッセージを行なうと、クレジット決済端末3001は、決済要求617を生成し、デジタル無線通信で、サービス提供システム1031に送信する。

〔0481〕図36 (f) に示すように、決済要求617は、メッセージが決済要求617であることを示すヘッダ情報、決済要求ヘッダ3642と、支払オフナー608と、支払オフナーへ送客609と、サービス提供システム1031が発行した照会番号3643と、この決済要求617の有効期限を示す有効期限3644と、担当者名3645と、ヤーチャントID3646と、この決済要求617を発行した日時を示す発行日時3647とから成るデータについて、ヤーチャントのデジタル署名を行ない、サービス提供者宛に封鎖化したものである。担当者名3646は、サービス提供者のオフショーンで設定する情報であり、設定されない場合もある。

〔0482〕サービス提供システム1031は、決済要求617を受信し、暗号を復号化し、デジタル署名をチェクして、決済要求617と支払要求613との内容を照合する。そして、決済処理手順テーブル3104を参照して、決済要求する決済処理手順を決定し、その決済処理手順の決済システム1031に、生成した決済要求619を送信する。

〔0483〕図37 (a) に示すように、決済要求619は、メッセージが決済要求619であることを示すヘッダ情報、決済要求ヘッダ3700と、ユーザが指定したサービスコードに対応するクレジットカード番号3701と、パーソナル・クレジット端末100が発行した要求番号3702と、支払金額3703と、支払オフナー3704と、ヤーチャントの口座番号を示すヤーチャント・アカウント番号3705と、クレジット決済端末3001が発行したトランザクション番号3706と、この決済要求619の有効期限を示す有効期限3707と、サービス提供者ID3708と、この決済要求619を発行した日時を示す発行日時3709とから成るデータについて、サービス提供者のデジタル署名を行ない、決済処理手順宛に封鎖化したものである。

〔0484〕決済システム1031は、決済要求619を受信し、暗号を復号化し、デジタル署名をチェクして、決済処理を行ない、決済完了通知620を生成し、サービス提供システム1031に送信する。

(50)

情報であり、設定されない場合もある。

〔0490〕サービス提供システム1031は、領収書623を受信し、暗号を復号化し、デジタル署名をチェクして、領収書624を生成し、デジタル無線電話通信で、パーソナル・クレジット端末100に送信する。

〔0491〕図38 (b) に示すように、領収書624は、メッセージが領収書624であることを示すヘッダ情報、領収書ヘッダ3812と、暗号を復号化した領収書3808と、決済処理手順のデジタル署名をしたユーザ向け決済情報3744と、サービス提供システム1031における処理に関する情報を示すサービス提供者処理情報3813と、サービス提供者ID3814と、この領収書624を発行した日時を示す発行日時3815とから成るデータについて、サービス提供者のデジタル署名を行ない、ユーザ宛に封鎖化したものである。サービス提供者処理情報3813は、サービス提供者のオフショーンで設定する情報であり、設定されない場合もある。

〔0492〕パーソナル・クレジット端末100は、領収書624を受信し、暗号を復号化し、デジタル署名をチェクして、その内容をLCD303に表示する。

〔0493〕次に、“キャンセル”の処理において、換算間で交換されるデータの内部の詳細について説明する。

〔0494〕図39 (a) ~ (f) は、“キャンセル”の処理において、交換するメッセージの内容を示している。

〔0495〕まず、ヤーチャントの担当者が、キャンセル操作300を行なうと、クレジット決済端末300は、キャンセル要求300を生成し、デジタル無線通信で、サービス提供システム1031に送信する。

〔0496〕一か、ユーザが、キャンセル操作300を行なうと、パーソナル・クレジット端末100は、キャンセル要求300を生成し、デジタル無線電話通信で、サービス提供システム1031に送信する。

〔0497〕図39 (a) に示すように、キャンセル要求300は、メッセージがキャンセル要求300であることを示すヘッダ情報、キャンセル要求ヘッダ3900と、暗号を復号化した決済完了通知3747と、このキャンセル要求300の有効期限を示す有効期限3901と、担当者名3902と、ヤーチャントID3903と、このキャンセル要求300を発行した日時を示す発行日時3904とから成るデータについて、ヤーチャントのデジタル署名を行ない、サービス提供者宛に封鎖化したものである。担当者名3902は、ヤーチャントのオフショーンで設定する情報であり、設定されない場合もある。

〔0498〕図39 (b) に示すように、キャンセル要求300は、メッセージがキャンセル要求300であることを示すヘッダ情報、キャンセル要求ヘッダ3900と、暗号を復号化した領収書3816と、このキャンセル要求300の有効期限を示す有効期限3910と、ユーザID3911と、この

(51)

キャンセル要求906を発行した日時を示す発行日時3912とから成るデータについて、ユーザのデジタル署名を行ない、サービス提供者宛に封書化したものである。

【0 4 9】 サービス提供システム102は、キャンセル要求902とキャンセル要求906とを受信し、それぞれ、暗号を復号化し、デジタル署名をチェックする。そして、要求番号とドラッグアクション番号とマーチャントIDとを照合して、キャンセル処理をしようとしているマーチャント及びユーザが、それぞれ、発行したキャンセル要求902とキャンセル要求906との対応をとり、さらに、キャンセル要求902とキャンセル要求906との内容を照合して、キャンセル要求907を生成し、決済システム103に送附する。

【0 5 0】 図3 (c) に示すように、キャンセル要求907は、メッセージがキャンセル要求907であることを示すヘッダ情報、キャンセル要求ヘッダ3917と、暗号を復号化した決済完了通知3727と、このキャンセル要求907の有効期限を示す有効期限3918と、サービス提供者1の発行日時3920とから成るデータについて、サービス提供者のデジタル署名を行ない、決済処理機関宛に封書化したものである。

【0 5 0 1】 決済システム103は、キャンセル要求907を受信し、暗号を復号化し、デジタル署名をチェックして、キャンセル処理を行ない、キャンセル完了通知908を生成し、サービス提供システム102に送附する。

【0 5 0 2】 図3 (d) に示すように、キャンセル完了通知908は、メッセージがキャンセル完了通知908であることを示すヘッダ情報、キャンセル完了通知ヘッダ3925と、決済システム103が行なったキャンセル処理をユニークに示す番号、キャンセル番号3928と、暗号を復号化して示す番号、キャンセル番号3928と、暗号を復号化したキャンセル要求3931と、決済処理機関のデジタル署名をしたサービス提供者向けキャンセル情報3927と、決済処理機関のデジタル署名をしたマーチャント向けキャンセル情報3938と、決済処理機関のデジタル署名をしたユーザ向けキャンセル情報3939と、決済処理機関ID 3930と、この決済完了通知を発行した日時を示す発行日時3931とから成るデータについて、決済処理機関のデジタル署名を行ない、サービス提供者宛に封書化したものである。サービス提供システム102は、キャンセル完了通知908を受信し、暗号を復号化し、デジタル署名をチェックして、キャンセル完了通知908とキャンセル処理機構910とを生成し、それぞれ、クレジット決済請求3930とバーソナル・クレジット請求100とに送附する。

【0 5 0 3】 図3 (e) に示すように、キャンセル完了通知909は、メッセージがキャンセル完了通知909であることを示すヘッダ情報、キャンセル完了通知ヘッダ3936と、キャンセル番号3937と、暗号を復号化したキャンセル要求3905と、決済処理機関のデジタル署名をしたマーチャント向け決済請求3928と、サービス提供システム

における処理に関する情報を示すサービス提供者処理情報3938と、サービス提供者ID 3939と、このキャンセル完了通知909を発行した日時を示す発行日時3940とから成るデータについて、サービス提供者のデジタル署名を行ない、マーチャント宛に封書化したものである。サービス提供者処理情報3938は、サービス提供者のオプションで設定する情報であり、設定されない場合もある。

【0 5 0 4】 図3 (f) に示すように、キャンセル処理情報910は、メッセージがキャンセル処理情報910であることを示すヘッダ情報、キャンセル処理情報ヘッダ3945と、キャンセル番号3946と、暗号を復号化したキャンセル要求3913と、決済処理機関のデジタル署名をしたユーザ向け決済情報3929と、サービス提供システムにおける処理に関する情報を示すサービス提供者処理情報3947と、サービス提供者ID 3948と、このキャンセル処理情報910を発行した日時を示す発行日時3949とから成るデータについて、サービス提供者のデジタル署名を行ない、ユーザ宛に封書化したものである。サービス提供者処理情報3947は、サービス提供者のオプションで設定する情報であり、設定されない場合もある。

【0 5 0 5】 クレジット決済請求300は、キャンセル完了通知909を受信し、暗号を復号化し、デジタル署名をチェックして、その内容をL D 302に表示する。一方、バーソナル・クレジット請求100も、キャンセル処理情報910を受信し、暗号を復号化し、デジタル署名をチェックして、その内容をL D 203に表示する。

【0 5 0 6】 次に、“顧客サービスコール”の処理において、機器間で交換されるデータの内容の詳細について説明する。

【0 5 0 7】 図4 0 (a) ~ (e) は、“顧客サービスコール”の処理において、交換するメッセージの内容を示している。

【0 5 0 8】 まず、マーチャントの担当者が、顧客サービスコール操作1200を行なうと、クレジット決済請求300は、顧客サービスコール要求1202を生成し、デジタル電話通話で、サービス提供システム102に送附する。

【0 5 0 9】 図4 0 (a) に示すように、顧客サービスコール要求1202は、メッセージが顧客サービスコール要求1202であることを示すヘッダ情報、顧客サービスコール要求4000と、ユーザを示す番号として、“決済”の処理の際に発行された顧客番号4001と、この顧客サービスコール要求をユニークに示す要求番号4002と、担当番号4003と、マーチャントID 4004と、この顧客サービスコール要求1202を発行した日時を示す発行日時4005とから成るデータについて、マーチャントのデジタル署名を行ない、サービス提供者宛に封書化したものである。担当番号4003は、マーチャントのオプションで設定する情報であり、設定されない場合もある。

【0 5 1 0】 サービス提供システム102は、顧客サービスコール要求1202を受信し、暗号を復号化し、デジタル

署名をチェックする。そして、サービス提供システム102は、顧客データベースからユーザを判定し、ユーザのアクセス制御情報と照合して、顧客サービスコール1203と顧客サービスコール要求1204とを生成し、それぞれ、ユーザのバーソナル・クレジット請求100とクレジット決済請求300とに送附する。

【0 5 1 1】 図4 0 (b) に示すように、顧客サービスコール1203は、メッセージが顧客サービスコール1203であることを示すヘッダ情報、顧客サービスコールヘッダ4010と、担当番号4011と、マーチャントID 4012と、マーチャント番号4013と、クレジット決済請求300が設定した要求番号4014と、サービス提供者ID 4015と、この顧客サービスコール1203を発行した日時を示す発行日時4016とから成るデータについて、サービス提供者のデジタル署名を行ない、ユーザ宛に封書化したものである。担当番号4011は、マーチャントのオプションで設定する情報であり、設定されない場合もある。

【0 5 1 2】 図4 0 (c) に示すように、顧客サービスコール要求1204は、メッセージが顧客サービスコール要求1204であることを示すヘッダ情報、顧客サービスコール要求1204が設定した要求番号4021と、サービス提供システム102からの応答メッセージ4022と、クレジット決済請求300が設定した要求番号4023と、サービス提供者ID 4024と、この顧客サービスコール要求1204を発行した日時を示す発行日時4025とから成るデータについて、サービス提供者のデジタル署名を行ない、マーチャント宛に封書化したものである。

【0 5 1 3】 クレジット決済請求300は、顧客サービスコール要求1204を受信し、暗号を復号化し、デジタル署名をチェックして、“呼び出し中”を表示する。

【0 5 1 4】 バーソナル・クレジット請求100は、顧客サービスコール1203を受信し、暗号を復号化し、デジタル署名をチェックして、ユーザに着信を知らせる。そして、ユーザが電話操作1207を行なうと、バーソナル・クレジット請求100は、着信応答1208をサービス提供システム102に送附する。着信応答1208を受信したサービス提供システム102は、呼び出し応答1210をクレジット決済請求300に送附し、クレジット決済請求300とバーソナル・クレジット請求100とは、通話状態になる。図4 0 (d) に示すように、着信応答1208は、メッセージが着信応答1208であることを示すヘッダ情報、着信応答ヘッダ4030と、クレジット決済請求300が設定した要求番号4031とによって構成され、呼び出し応答1210は、図4 0 (e) に示すように、メッセージが呼び出し応答ヘッダ4032であることを示すヘッダ情報、呼び出し応答ヘッダ4033と、クレジット決済請求300が設定した要求番号4033とによって構成される。

【0 5 1 5】 次に、“問い合わせコール”の処理において、機器間で交換されるデータの内容の詳細について説明する。

(52)

【0 5 1 6】 図4 1 (a) ~ (e) は、“問い合わせコール”の処理において、交換するメッセージの内容を示している。

【0 5 1 7】 まず、ユーザが、問い合わせコール操作1213を行なうと、バーソナル・クレジット決済請求100は、問い合わせコール要求1215を生成し、デジタル電話通話で、サービス提供システム102に送附する。

【0 5 1 8】 図4 1 (a) に示すように、問い合わせコール要求1215は、メッセージが問い合わせコール要求1215であることを示すヘッダ情報、問い合わせコール要求ヘッダ4100と、マーチャントID 4101と、担当番号4102と、この問い合わせコール要求をユニークに示す要求番号4103と、ユーザID 4104と、この問い合わせコール要求1215を発行した日時を示す発行日時4105とから成るデータについて、ユーザのデジタル署名を行ない、サービス提供者宛に封書化したものである。担当番号4103は、“決済”の処理の際に、マーチャントのオプションで設定する情報であり、設定されない場合もある。

【0 5 1 9】 サービス提供システム102は、問い合わせコール要求1215を受信し、暗号を復号化し、デジタル署名をチェックする。そして、サービス提供システム102は、問い合わせコール1216と問い合わせコール要求1217とを生成し、それぞれ、マーチャントのクレジット決済請求300とバーソナル・クレジット決済請求100とに送附する。

【0 5 2 0】 図4 1 (b) に示すように、問い合わせコール1216は、メッセージが問い合わせコール1216であることを示すヘッダ情報、問い合わせコールヘッダ4110と、顧客番号4111と、バーソナル・クレジット請求100が設定した要求番号4112と、サービス提供者ID 4113と、この問い合わせコール1216を発行した日時を示す発行日時4114とから成るデータについて、サービス提供者のデジタル署名を行ない、マーチャント宛に封書化したものである。

【0 5 2 1】 図4 1 (c) に示すように、問い合わせコール要求1217は、メッセージが問い合わせコール要求1217であることを示すヘッダ情報、問い合わせコール要求ヘッダ4120と、サービス提供システム102からの応答メッセージ4121と、バーソナル・クレジット決済請求100が設定した要求番号4121と、サービス提供者ID 4122と、この問い合わせコール要求1217を発行した日時を示す発行日時4123とから成るデータについて、サービス提供者のデジタル署名を行ない、ユーザ宛に封書化したものである。

【0 5 2 2】 バーソナル・クレジット請求100は、問い合わせコール要求1217を受信し、暗号を復号化し、デジタル署名をチェックして、“呼び出し中”を表示する。クレジット決済請求300は、問い合わせコール1216を受信し、暗号を復号化し、デジタル署名をチェックして、マーチャントに着信を知らせる。そして、マーチャ



ントが電話操作1220を行なうと、クレジット決済額5000は、貸出客1221をサーチして提供システムに送附する。着信客1221を受信したサーチ提供システムは、呼び出し客1222をバリエット・クレジット端末に送附し、バリエット・クレジット端末100とクレジット決済額500とは、電話状態になる。

「0523」 図4 1 (d) に示すように、着信応答1231は、メッセージが着信応答1231であることを示すヘッダ情報、着信応答ヘッダ1138と、パーティクル・クルシット技術宛先1004の宛定した要求番号1139とによって構成され、呼び出し応答1231は、図4 1 (e) に示すように、メッセージが呼び出し応答1231であることを示すヘッダ情報、呼び出し応答ヘッダ1130と、パーティクル・クルシット技術宛先1004の宛定した要求番号1131とによって構成される。

【0524】(実施の形態2)次に、本発明の第2の実施形態について説明する。第2の実施形態では、パーソナル・リモート・クレジット決済サービスとの処理の効率化を可能にするパーソナル・リモート・クレジット決済システムについて説明する。

10562.] このバーナル・リモート・クレジット決済システムの基本的な構成は、第1の処理部と同じである。図1に示すように、2系統の光導線通信機能と電子的なクレジットカード機能とを持つバーナル・クレジット端末100と、小売販売店におけるクレジット決済処理を行なうクレジット決済処理店におけるバーセルを含む決済処理会社におけるクレジット決済処理を行なうクレジット端末101と、バーナル・クレジット端末100、クレジット決済処理店101及びクレジット端末103を結ぶ通信ネットワークの中心に位置してバーナル・リモート・クレジット決済サービスを提供するサービス提供システム102と、ネットワークにおけるデータ伝送路を提供するデジタル公衆網108と、バーナル・クレジット端末100とデジタル公衆網101に接続する基盤設備の基体100とを備えている。

【0526】パーソナル・クレジット端末100は、海外  
銀とデジタル無線電話との2系統の双方向無線通信機能  
と、電子的なクレジットカードの機能を持つ携帯無線  
電話端末である。また、小売販売店におけるクレジット  
決済処理を行なうクレジット決済装置101も、該無線通  
信とデジタル無線電話との2系統の双方向通信機能を持  
つ。

[0562] なお、図1において、105は「ペーパナル  
レスリット」通米10とチタリ技術装置10との間で  
行なわれる鉄道通過の伝送路、106は、「ペーパナル・カ  
シラ」通米100と基地局10との間で行なうデジタル無線  
通信の伝送路を示し、107は、基地局10とデジタル公衆網  
108とを結ぶデジタル通信回線、109は、デジタル公衆  
網108とネットエッジ装置101とを結ぶデジタル通信  
回線、110は、ペーパナルシステム102とを結ぶデジタル通信

108とを結ぶデジタル電話通信回路111は、サービス提供システム102と決済システム103とを結ぶデジタル通信回路を示している。特に、デジタル通信回路109とデジタル通信回路111は、多重化によって、複数の通信回路として動作する。

【0528】バーソナル・リモート・クレジット決済サービス  
の通常の運用形態は、第1の実施形態と同じである。次のような形態となる。

【0529】 茨城システム101は、クレジットカード会社  
社または決済処理会社、にクレジット・決済装置101は、  
小売販売店に設置され、バーナクル・クレジット端末10  
は、消費者が持ち歩く、サージと提供システム101は、  
バーナクル・リモート・クレジット決済サービスを提供  
する会社に設置され、クレジットカード会社がバーナク  
ル・リモート・クレジット決済サービスを提供する場合  
には、サージと提供システム101は、クレジットカード  
会社には提供される。

10633) また、前提として、消費者は、クレジットカーディンレットとの間で、クレジットサービスとの会員契約を、パーソナル・リモート・クレジット決済サービスを提供する会社との間では、パーソナル・リモート・クレジット決済サービスとの会員契約を、さらに、電話会社との間で、無線電話サービスとの契約を結んでいる。同様に、小売販売店も、クレジットカード会社との間で、クレジットサービスとの加盟店契約を、パーソナル・リモート・クレジット決済サービスを提供する会社との間で、パーソナル・リモート・クレジット決済サービスとの加盟店契約を、さらに、電話会社との間で、デジタル電話サービスとの契約を結んでいる。

「0533」また、パーソナル・リモート・テレビジョン技術サービスが、テレビジョンカード会社とは別会社によって提供される場合には、パーソナル・リモート・テレビジョン技術サービスを提供する会社は、1社または複数テレビジョンカード会社との間で、テレビジョンサービスに提供している金目に対して、テレビジョンカード会社の代わりに、電子的なテレビジョンカードを発行し、パーソナル・リモート・テレビジョン技術サービスを運営する契約を結ぶことになる。

【0532】また、決済処理会社が、決済システム103を用いてクレジット決済処理を行なう場合には、決済処理会社は、1社または複数のクレジットカード会社との間で、クレジット決済処理を決済処理会社が代行する契約を結んでいる。

【0533】なお、クレジットカードによって、クレジット決済処理を行なう決済システムが異なる場合には、図1の決済システム103と同様の形態で、複数の決済システムが、サービス提供システム102にデジタル通信回線によって接続される。

【0534】以下では、本システムの説明を簡単にするために、パーソナル・コンピュータ端末100の所有する消

乗客エグゼクティブ、クレジット決済係員10人を配置し、大がかりな店をマニージャークレリック、クレジット決済係員10人を操作する販売店員を担当者（Operator）、パソナル・リモテ・クレジット決済サービスを提供する会社をサービス提供者（Service Provider）、決済システム103を用いたクレジット決済処理を行うクレジットカード会社または決済処理会社は決済処理機関（Transaction Processor）と呼ぶこととする。

【0535】本システムでは、ユーザがマージヤントに  
対して商品の代金をクレジットによって支払う場合、バ  
ーソナル・クレジット端末100、クレジット決済装置101  
及びサビエス提供システム103の三者間で電子的に決済  
情報を交換し、さらに、サビエス提供システム102と決  
済システム103との間で電子的に決済情報を交換するこ  
とによって、クレジット決済処理を行なう。

【0536】基本的には、サービスタ提供システム101が、パーソナル・クライアント端末100とクライアント・決済装置101とから、それぞれ、支払要求と決済要求とを受け取り、支払要求と決済要求とを照合し、ユーザとマシントとに代わって、決済システム101に決済処理を要求する。そして、決済システムが実際の決済処理を行なう。

【053】この時、パーソナル・タブレット端末100とタブレット装置101とは、伝送路106を用いて、外部装置を行ない、パーソナル・タブレット端末100とサーバ提供システム102とは、伝送路106及び基地局104、さらに、タブレット装置107、タブレット公衆網108及びタブレット電話109を行ない、タブレット無線装置101によるサーバ提供システム102とは、タブレット電話装置101とサーバ提供システム102とは、タブレット電話装置109を通じてタブレット電話108及びタブレット通信109を行ない、サーバ提供システム102とタブレット103とは、タブレット通信1011を通じて、タブレット端末100と通信を行う。

【0538】パーソナル・ケルジット端末100とサービ  
ス提供システム101との通信、ケルジット決済装置101と  
サービス提供システム102との通信、及び、サービス提  
供システム103と決済システム103との通信では、交換さ  
れる決済情報と、全て、暗号化して通信する。暗号化に  
よる、秘密鍵方式の暗号処理と公開鍵方式の暗号処理とを  
組み合わせて、情報を電子封鎖化して通信する。

【0539】次に、本システムを構成する各構成要素について説明する。

【0540】まず、バーソナル・クレジット端末100について説明する。バーソナル・クレジット端末100の外観は、第1の実施形態と同じであり、図2(a)及び図2(b)に示す前面側及び背面側の外観を有している。

【0541】このパーソナル・クレジット端末100には、クレジットカードモードとデジタル無線電話モード、個人情報管理モードの3つの動作モードがあり、モ

ードスアイチ2004によって与えられる、パーソナル・クライアント用100は、デジタル無線電話モードでは、デジタル無線電話として動作し、クライアントモードでは、デジタル無線電話として動作し、つまり、電子的なクライアント手段、つまり、電子的なクライアントとして動作する。

【0542】電子的なクライアントは、ユーザにより、あるネットワーク会社と他のネットワークサービスの会費契約を前提として、パーソナル・クライアント用100に

登録されているユーザが、複数のクレジットカードの会員資格を保持している場合には、複数のクレジットカードが、バーチャル・クレジット・端末100に登録される。

[0543] 個人情報管理モードは、バーチャル・クレジット・端末100の内部に格納されるユーザの個人情報を管理する動作モードであり、個人情報管理モードにおいて、ユーザは、登録されている個人情報や写真カード等の参照、及び、ユーザ設定情報の設定を行なう。

【0544】このバージョン・クレジット増額100を用いて、例えば電話をかける場合には、ユーザは、まず、モードスイッチ204で、動作モードをデジタル無線電話モードにし、次に、テンキー・スイッチ208で電話番号を入力して、通話スイッチ205を押す。以上の操作で、ユーザは、入力した電話番号に電話をかけることが出来る。

【05445】また、バーソナル・クレジット端末100に通常の電話がつかつて来た場合には、バーソナル・クレジット端末100は、その時の動作モードに関係なく、受信音を受取る。この場合には、通常のインテリジェントなことで自動的にデジタリ無線電話モードに切り替わり、ユーザは電話を受けることが出来る。

【054】また、サーチメントにクレジットで代金を支払う場合には、まず、モータースイッチ04にのみ動作モードをクレジットカードモードに設定し、フアンクションスイッチ207で、支払に使用するクレジットカード番号を選択する。次に、デビーススイッチ308で、支払金額をを入力し、赤外線送信器120をサーチメントのクレジット決済装置100の方向に向けて、実行スイッチ05を押す。以上の操作によって、パーソナル・クレジット端末100は、クレジット決済装置101との間で無線通信を行ない、それとともにサーチ機スイッチ50と102との間でデジタル無線電話通信を行ない、それぞれが決済情報とを交換し、クレジット決済処理を行なう。

【0547】次に、クレジット決済装置101について説明する。クレジット決済装置101の外観は、第1の実施

形態と同じであり、図3に示す外観を有している。  
[0548] このクレジット状誘導索500には、クレジ  
ット状誘導ボードとデジタル電話モード、マニピュ  
レーションボードの3つの動作モードがあり、モードスイ  
ッチ504によって切替る。デジタル電話モードでは、デ  
ジタル電話機として動作し、クレジット状誘導ボードで  
は、パーソナル・リモート・クレジット状誘導ボードとの

(55)

クレジット決済処理端末として動作する。

〔0549〕 マーチャント情報管理モードは、クレジット決済端末300の内部に格納されるマーチャントの情報管理する動作モードであり、マーチャント情報管理モードにおいて、マーチャントは、登録されているマーチャント情報等の参照、及び、マーチャント設定情報の設定を行なう。

〔0550〕 このクレジット決済端末300から、例えば電話番号をかける場合には、担当者は、まず、モースイッチ304で、動作モードをデジタル電話番号モードにし、次に、テンキースイッチ307で電話番号を入力する。以上の操作によって、担当者は、入力した電話番号に電話をかけることができる。

〔0551〕 また、クレジット決済端末300に通常の電話がかかって来た場合には、クレジット決済端末300は、動作モードに切換なく、着信音を発する。この場合には、電話器303を上げるか、フックスイッチ305を押すことで、自動的に電話モードに切り替わり、担当者は電話を受けることができる。

〔0552〕 また、クレジット決済処理を行なう場合には、まず、キャッシュレジスタ311で、商品価格と税金等から合計金額を計算し、その金額をユーザに伝える。次に、クレジットによる支払を希望するユーザの要望にしたがって、キャッシュレジスタ311のクレジット決済スイッチ312を押し、ユーザがパーソナル・クレジット端末100で代金の支払操作を行なうのを待つ。ユーザが、代金の支払操作を行なうと、ユーザが入力した支払金額がLCD303に表示される。さらに、ユーザの信用照会の結果が表示される。担当者はその内容を確認して、実行スイッチ308を押す。

〔0553〕 以上の操作によって、クレジット決済装置101は、パーソナル・クレジット端末100、及びサービス提供システム102と、それぞれ、決済情報を交換して、クレジット決済処理を行なう。

〔0554〕 次に、サービス提供システムについて説明する。サービス提供システム103は、第1の実施形態と同様のブロック構成を具備し、図4に示すように、パーソナル・リモート・クレジット決済サービスにおいて、パーソナル・クレジット端末100、クレジット決済装置101、及び決済システム103のそれぞれと交換する決済情報のデータ処理とその際のデータ通信の制御とを行なうサービスサーバ400と、ユーザ、マーチャント、及び決済処理装置に関する属性情報とサービス提供システム103が提供したサービスの履歴情報とを管理するサービス・ディレクタ情報サーバ401と、ユーザの属性情報とパーソナル・クレジット端末100内のデータとを管理するユーザ情報サーバ402と、マーチャントの属性情報とクレジット決済端末300内のデータとを管理するマーチャント情報サーバ403と、決済処理装置の属性情報と決済処理の履歴情報とを管理する決済処理装置情報サーバ404

4と、サービス提供者がサービス提供システム103の運用管理を行なう管理システム407とを備えており、各サーバ400～404及び管理システム407が、それぞれ1台または複数台のコンピュータで構成されている。

〔0555〕 また、サービスサーバ400、サービス・ディレクタ情報サーバ401、ユーザ情報サーバ402、マーチャント情報サーバ403及び決済処理装置情報サーバ404は、それぞれ、ATM-LANケーブル409、410、411、412、413によってATM-LANスイッチ405に接続され、サービスサーバ400は、ATM-LANスイッチ405を介して、サービスディレクタ情報サーバ401、ユーザ情報サーバ402、マーチャント情報サーバ403、または決済処理装置情報サーバ404にアクセスする。

〔0556〕 また、ATM-LANスイッチ405は、ATM-LANケーブル415によって、ATM交換機406に接続される。ATM交換機406には、デジタル公衆網100と結ぶデジタル通信回線109と、決済システム103と結ぶデジタル通信回線111とが接続され、サービスサーバ400は、ATM-LANスイッチ405及びATM交換機406を介して、パーソナル・クレジット端末100、クレジット決済装置101、及び決済システム103と通信を行なう。

〔0557〕 管理システム407は、ATM-LANケーブル414によって、ATM-LANスイッチ406に接続され、さらに、ATM-LANケーブル418によって、ATM交換機406に接続される。管理システム407は、ATM-LANスイッチ408、ATM交換機406、及びATM-LANスイッチ405を介して、サービスサーバ400、サービスディレクタ情報サーバ401、ユーザ情報サーバ402、マーチャント情報サーバ403、または決済処理装置情報サーバ404にアクセスして、サービス提供システム103の運用管理を行なう。

〔0558〕 ATM交換機406は、サービス提供システム102の外部と内網との通信、及びサービス提供システム102の内網間の通信において、データ通信の交換機として動作する。また、ATM交換機406は、複数の通信方式に対応し、通信アダプタの機能を有する。例えば、サービスサーバ400とクレジット決済装置101との通信では、まず、クレジット決済装置101とATM交換機406との間で、ISDNのデータパケットを交換し、ATM交換機406が、ISDNのデータパケットからATMパケットへの変換、及び、その逆変換を行なう。ATM交換機406とサービスサーバ400との間で、ATMパケットを交換する。同時に、サービスサーバ400とパーソナル・クレジット端末100との間の通信、サービスサーバ400と決済システム103との間の通信においても、ATM交換機406が、それぞれの通信方式に対応して、通信データの交換を行なう。

〔0559〕 また、パーソナル・クレジット端末100～サービス提供システム102間、及び、クレジット決済装置101～サービス提供システム103間の通信費用を軽減す

(56)

るため、通常、サービス提供システム103は、パーソナル・リモート・クレジット決済サービスを提供する地域(サービスエリア)ごとに設置される。したがって、ATM交換機406には、他の地域のサービス提供システムと結ぶ専用デジタル通信回線417が接続される。この場合、サービス提供システム102同士は、お互いにデータを共有し、協調してデータ処理を行なう。

〔0560〕 サービス提供システム間のデータの共有、協調処理の仕組みに関しては、後で詳しく説明する。決済システム103は、第1の実施形態と同様に、図5に示すブロック構成を備えている。パーソナル・リモート・クレジット決済サービスにおいて、決済システム103が行なうクレジット決済処理は、サービス提供システム103からの決済要求に対して、トランザクション処理サーバ500が、加入者情報サーバ501、加盟店情報サーバ502、及び取引情報サーバ503の情報を、それぞれ更新することによって成立する。

〔0562〕 また、ATM交換機505には、サービス提供システム103と結ぶデジタル通信回線515、さらにオンラインシステムと結ぶ銀行専用回線516、さらに、他の決済処理装置の決済システムと結ぶ専用デジタル回線518が接続され、決済システム103は、銀行オンラインシステム、及び、他の決済処理装置の決済システムと通信を行ない、金融機関間の決済処理を行なう。

〔0563〕 管理システム508は、ATM-LANケーブル512によって、ATM-LANスイッチ507に接続され、さらに、ATM-LANケーブル514によって、ATM交換機505に接続される。管理システム508は、ATM-LANスイッチ507、ATM交換機505、及びATM-LANスイッチ504を介して、トランザクション処理サーバ500、加入者情報サーバ501、加盟店情報サーバ502、及び取引情報サーバ503にアクセスし、決済システム103の運用管理を行なう。

〔0564〕 ATM交換機505は、決済システム103の外部と内網との通信、及び決済システム103の内網間の通信において、データ通信の交換機として動作する。また、ATM交換機505は、複数の通信方式に対応した、通信アダプタの機能を有し、トランザクション処理サーバ500とサービス提供システム103との間の通信、トランザクション処理サーバ500と銀行オンラインシステムとの間の通信、トランザクション処理サーバ500と他の決済処理装置の決済システムとの間の通信において、ATM交換機505が、それぞれの通信方式に対応して、通信データの交換を行なう。

〔0565〕 次に、本システムが提供するパーソナル・リモート・クレジット決済サービスについて説明する。〔0566〕 パーソナル・リモート・クレジット決済サービスには、大きく分けて、“決済”、“キャンセル”、“顧客サービスコール”、及び“問い合わせコー

ル”の4つ処理がある。

〔0567〕 “決済”は、ユーザがマーチャントに代金をクレジットで支払うクレジット決済を、クレジットカードや利用明細書などを、直接受け渡すことなく、無断値によって行なう処理。“キャンセル”は、パーソナル・リモート・クレジット決済サービスの“決済”の処理によって完了した取引を、ユーザとマーチャントとの同意の基に、無断値によって、取り消す処理。“顧客サービスコール”は、パーソナル・リモート・クレジット決済サービスの“決済”の処理によって取引のあったユーザに対して、マーチャントがユーザの電話番号を知らない場合でも、電話連絡を可能にする処理。そして、“問い合わせコール”は、パーソナル・リモート・クレジット決済サービスの“決済”の処理によって取引のあったマーチャントに対して、ユーザが自分の電話番号を知られることなく、問い合わせの電話を可能にする処理である。

〔0568〕 このパーソナル・リモート・クレジット決済サービスにおける“決済”の処理の流れを図43に示し、また、この“決済”処理の際の、パーソナル・クレジット端末100のLCD303の表示例を図44の(a)～(1)に示し、クレジット決済端末300のLCD302の表示例を図8の(a)～(g)に示している。

〔0569〕 また、このパーソナル・リモート・クレジット決済サービスにおける“キャンセル”処理の流れを図9に示し、また、この“キャンセル”処理の際の、パーソナル・クレジット端末100のLCD203の表示例を図10の(a)～(h)に示し、クレジット決済端末300のLCD303の表示例を図11の(a)～(g)に示している。

〔0570〕 また、このパーソナル・リモート・クレジット決済サービスにおける“顧客サービスコール”の処理の流れを図45(a)に示し、また、この“顧客サービスコール”処理の際の、パーソナル・クレジット端末100のLCD203の表示例を図13の(a)～(h)に示し、クレジット決済端末300のLCD302の表示例を図14の(a)～(g)に示している。

〔0571〕 また、このパーソナル・リモート・クレジット決済サービスにおける“問い合わせコール”の処理の流れを図45(b)に示し、また、この“問い合わせコール”処理の際の、パーソナル・クレジット端末100のLCD303の表示例を図13の(b)～(f)に示し、クレジット決済端末300のLCD302の表示例を図14の(h)～(i)に示している。

〔0572〕 これらの各処理の流れは、実質的に、第1の実施形態で説明したものと同一である。〔0573〕 次に、パーソナル・クレジット端末100の内蔵構成を説明する。〔0574〕 図15(a)は、パーソナル・クレジット端末100のブロック構成図である。この端末は、ROM、





(59)

【0590】チャンネルコーデック1513は、こうした動作を行なうために、図46に示すように、ターミナル1Dを格納する1Dレジスタ(ID)21605と、チャンネルコーデック1513の動作を制御するチャンネルコーデック制御レジスタ(CONTROL)21606と、音声コーデック1513から入力されるデジタル音声データを格納する音声送信バッファ21607と、受信データのなかから抽出したデジタル音声データを格納する音声受信バッファ21608と、制御レジスタ1508を介してCPU1500から入力されるデータ通信データを格納するデータ送信バッファ21609と、受信データのなかから抽出したデータ通信データを格納するデータ受信バッファ21610とを具備している。

【0591】制御レジスタ1514は、チャンネルコーデック1513に、音声送信バッファ21607と音声受信バッファ21608への、音声コーデック1513による書き込みと読み出しとの動作を示す制御値であり、音声コーデック1513は、制御レジスタ1514をローレベルにして、音声送信バッファ21607にデジタル音声データを書き込み、制御レジスタ1514をハイレベルにして、音声受信バッファ21608からデジタル音声データを読み出す。

【0592】制御レジスタ1551は、チャンネルコーデック1513に、データ送信バッファ21609とデータ受信バッファ21610への、制御レジスタ1508を介したCPU1500による書き込みと読み出しの動作を示す制御値であり、制御レジスタ1551をローレベルにして、データ送信バッファ21609にデータ通信データを書き込み、制御レジスタ1551をハイレベルにして、データ受信バッファ21610からデータ通信データを読み出す。

【0593】変調レジスタ1514は、チャンネルコーデック1513から入力するシリアル・デジタル信号1547を、PLL1516から供給される発振電圧信号1552をベースバンドとするアナログ送信信号1549に変換し、RF部へ供給する。RF部へ供給されたアナログ送信信号1549は、無線電波として、アンテナ201から出力される。

【0594】逆に、無線電波をアンテナ201が受信すると、RF部151から復調レジスタ1515にアナログ受信信号1550が入力される。復調レジスタ1515は、PLL1516から供給される発振電圧信号1553を、アナログ受信信号1550のベースバンドとして、アナログ受信信号1550を復調して、シリアル・デジタル信号1548を、チャンネルコーデック1513へ供給する。

【0595】また、バッテリリチャージ量を検出するバッテリリチャージ検出部1518は、パーソナル・クレジット端末100の容量検出部1518は、CPU1500によって設定された値Q(Q>0)以下になった時に、送信信号1557をアサートする。送信信号1557は、CPU1500にRAM1502上のデータのバックアップ処理を促す送信信号であり、Qは、パーソナル・クレジット端末100が、サービス提供システム102と通信して、RAM1502上のデータを、サービス提供システム102にバックアップする処理(デー

タバックアップ処理)を行なうのに十分な値である。

【0596】また、制御レジスタ1508は、図46に示すように、その内部に、フレームカウンタ(FRAME)21600、起動フレームレジスタ(FRAME)21601、クロックカウンタ(CLOCK)21602、アップデート時刻レジスタ(UPDATE)21603、及び新レジスタ(INT)21604の5つのレジスタを内蔵する。

【0597】フレームカウンタ21600は、デジタル無線電話のフレーム数をカウントするカウンタ、起動フレームレジスタ21601は、次の起動するフレーム番号を格納するレジスタ、クロックカウンタ21602は、現在の日付と時刻をカウントするカウンタ、アップデート時刻レジスタ21603は、パーソナル・クレジット端末100が、サービス提供システム102と通信して、RAM1502上のデータを更新する処理(データアップデート処理)を行なう時刻を格納するレジスタ、そして、新レジスタ21604は、CPU1500への新送の要因を示すレジスタである。

【0598】一般に、デジタル無線電話では、デジタル無線電話の制御チャンネルの制御データを周期的に受信し、ターミナル1Dと照合することによって、自分宛の電話の着信を実現している。このパーソナル・クレジット端末100では、フレームカウンタ21600と起動フレームレジスタ21601とを用いて、制御データの同次受信を行なう。すなわち、起動フレームレジスタ21601に、次回に起動するフレーム番号を格納しておき、フレームカウンタ21600がカウンタアップして、起動フレームレジスタ21601の値に等しくなった時、制御レジスタ1508が、アドレス・データ信号線1558を介して、チャンネルコーデック1513、PLL1516、及びRF部1517を起動し、制御データの受信を行なう。

【0599】また、制御レジスタ1508は、クロックカウンタ21602の値が、アップデート時刻レジスタ21603の値に一致した場合と、新送信号1538、1554、1557のいずれかの新送信号がアサートされた場合に、その新送要因を、新レジスタ(INT)21604に設定して、新送信号1519をアサートし、CPU1500に新送処理を促す。CPU1500は、新送処理で、新レジスタ(INT)21604を読みだし、その新送要因に応じた処理を行なう。

【0600】この新レジスタ(INT)21604のビットフィールドは、図47(a)に示すように意味づけられている。この意味づけは、第1の実施形態において、図18(b)を用いて説明したものと同じである。

【0601】次に、RAM1502に格納されるデータに関して説明する。

【0602】図48は、RAM1502に格納されるデータのRAMマップの模式図である。

ある。基本プログラム領域21800は、ROM1501に格納されているプログラムのバージョンアップされたモジュール、及び、パッチプログラムや、追加プログラムが格納される。

【0604】ユーザ領域21802は、ユーザが自由に使用できる領域、ワーク21803領域は、CPU100がプログラムを実行する際に使用する作業領域、また、テンポラリ領域21804は、パーソナル・クレジット端末100が受信した情報を一時的に格納する領域である。サービスデータ領域21801は、パーソナル・リモート・クレジット決済サービスの1D情報や、クレジットカード情報、履歴情報などを格納する領域であり、この領域のデータは、サービス提供システム102によって管理される。

【0605】サービスデータ領域21801には、さらに、データ管理情報21805、個人情報21806、写真データ21807、ユーザ設定情報21808、電話情報21809、クレジットカードリスト21810、利用履歴リスト21811、及び実施データ領域21812の8つの領域がある。データ管理情報21805は、サービスデータ領域21801に格納されている情報の管理情報を格納する領域、個人情報21806は、ユーザの年齢、性別等の情報を格納する領域、写真データ領域21807は、ユーザの顔写真のデータを格納する領域、ユーザ設定情報21808は、パーソナル・リモート・クレジット決済サービスに関するユーザの設定情報を格納する領域、電話情報21809は、デジタル無線電話に関する情報を格納する領域、クレジットカードリスト21810は、ユーザが登録したクレジットカードのリスト情報と、ユーザが登録したクレジットカードのリスト情報とを格納する領域、利用履歴リスト21811は、パーソナル・リモート・クレジット決済サービスの利用履歴情報を格納する領域、実施データ領域21812は、他の7つの領域で管理されている情報の実データデータを格納する領域である。

【0606】次に、サービスデータ領域21801に格納される情報について詳しく説明する。

【0607】図49は、サービスデータ領域21801に格納される情報の関係性を詳細に示した模式図である。

【0608】データ管理情報21805は、アップデート日時21900、次回アップデート日時21901、ターミナル・ステータス21902、個人情報アドレス21903、写真データアドレス21904、ユーザ設定情報アドレス21905、電話情報アドレス21906、クレジットカードリスト・アドレス21907、及び利用履歴リスト・アドレス21908の9つの情報によって構成される。

【0611】ターミナル・ステータス21902は、パーソナル・クレジット端末100の状態を示し、個人情報アドレス21903、写真データアドレス21904、ユーザ設定情報アドレス21905、電話情報アドレス21906、クレジットカードリスト・アドレス21907、及び利用履歴リスト・アドレス21908は、それぞれ、個人情報21806、写真データ21807、ユーザ設定情報21808、電話情報21809、クレジットカードリスト21810、利用履歴リスト21811が格納されている領域の先頭番地を示す。

【0612】電話情報21809は、さらに、発信電話番号21909、電話情報アドレス21910、短縮ダイヤル設定ファイル・アドレス21911の3つの情報によって構成される。発信電話番号21909は、ユーザが、前回、かけた電話の電話番号を示し、この情報は、デジタル無線電話の再送時に用いられる。電話情報アドレス21910と短縮ダイヤル設定ファイル・アドレス21911とは、それぞれ、電話情報、短縮ダイヤル設定ファイルが格納されている実データデータ領域上のアドレスを示す。

【0613】クレジットカードリスト21810には、ユーザが登録したクレジットカードのリスト情報が格納されている。クレジットカードリスト21810では、一つのクレジットカードに対して、クレジットカード名21912(21919)、クレジットカード番号21913(21920)、有効期限21914(21921)、クレジットカード・ステータス21915(21922)、イメージ・データ・アドレス21916(21923)、オブジェクト・データ・アドレス21917(21924)、及びアクセス時刻21918(21925)の7つの情報が格納されている。

【0614】クレジットカード・ステータス21915(21922)は、クレジットカードが有効か否か、及び、利用限度額を示し、イメージ・データ・アドレス21916(21923)は、クレジットカードのイメージデータが格納されている実データデータ領域21812上のアドレスを示す。オブジェクト・データ・アドレス21917(21924)は、そのクレジットカードのプログラムのオブジェクト・データが格納されているアドレスを示し、アクセス時刻21918(21925)は、ユーザがそのクレジットカードを利用した最新の時刻を示す。

【0615】オブジェクト・データ・アドレス21917(21924)には、実データ領域21812上のアドレスを示すローカルアドレス、または、サービス提供システム102のユーザ情報サーバ1402上のアドレスを示すリモートアドレスが格納される。オブジェクト・データ・アドレス21917(21924)にリモートアドレスが格納されている場合、ユーザが、そのクレジットカードを選択し、利用しよう

(60)

(61)

とすると、パーソナル・クレジット端末100は、サービス提供システム102からオプジェクト・データをダウンロードし、クレジットカードのプログラムを実行する。クレジットカードを表示するだけでは、イメージ・データ・プログラム1916(1933)によって示される媒体データ領域21812のイメージデータが提示され、オプジェクト・データのダウンロードは行なわれない。

[0616] このオプジェクト・データ・プログラム1917(1933)に格納されるアドレスは、サービス提供システム102によって決定される。データアップロード処理の際に、各クレジットカードのアクセス時刻を比較し、アクセス時刻が最近のクレジットカードに、ローカルアドレスが割り当てられる。但し、媒体データ領域21813の容量に余裕がある場合には、全てのクレジットカードのオプジェクト・データ・アドレスが、ローカルアドレスである場合もある。

[0617] 利用履歴リスト21811では、一つのパーソナル・リモート・クレジット決済サービスの利用に対して、要求番号19126(1930)、サービスコード21917(1931)、利用時刻19128(1932)、及び利用情報アドレス21929(1933)の4つの情報格納される。

[0618] 要求番号19126(1930)は、サービスととの取引を(ユーザから見て)ユニークに示す番号であり、支払オプジェクト608を生成する際に、パーソナル・クレジット端末100が実行する番号、サービスコード21917(1931)は、利用したクレジットカードサービスの種類を示すコード番号、利用時刻19128(1932)は、パーソナル・リモート・クレジット決済サービスを利用した時刻、利用情報アドレス21929(1933)は、領収書、または、利用内容を示す情報が格納されているアドレスを示す。

[0619] 利用情報アドレス21919(1933)には、媒体データ領域21812上のアドレスを示すローカルアドレス、または、サービス提供システム102のユーザ情報データベース上のアドレスを示すリモートアドレスが格納される。

[0620] 利用情報アドレス21919(1933)に、リモートアドレスが格納されている場合、ユーザが、その利用履歴情報をアクセスすると、パーソナル・クレジット端末100は、サービス提供システム102から、利用情報をダウンロードし、領域21804にダウンロードして(リモートアクセス)、LCD203に表示する。

[0621] 利用情報アドレス21919(1933)に格納されるアドレスもまた、サービス提供システムによって決定される。データアップロード処理の際に、各利用情報の利用時刻を比較し、利用時刻が最近の利用情報に、ローカルアドレスが割り当てられる。但し、媒体データ領域21813の容量に余裕がある場合には、全ての利用情報アドレスが、ローカルアドレスである場合もある。

[0622] 次に、CPU1500が行なう処理について説明する。

[0623] 図51は、CPU1500が行なう処理フローの概念図である。

[0624] 図51に示すように、CPU1500が行なう処理には、メインルーチン21109と、前記処理ルーチン21122の2つの処理ルーチンがあり、メインルーチンは、送信データ及び受信データの処理、並びに、他の構成要素の制御を行なう処理ルーチンである。メインルーチンからは、外部割込によって要求されるプロセス(処理)を抽出する処理ルーチンである。したがって、CPU1500は、通常、メインルーチンの処理を行なう。前記信号1916がスタートされると、CPU1500は、メインルーチンから前記処理ルーチンへ飛び、前記処理を行ない、前記処理を終了すると、メインルーチンに戻り、元のメインルーチンの処理を再開する。

[0625] CPU1500が、メインルーチンの中で実行するプロセスは、17種類のプロセスであり、CPU1500は、プロセスを動的に選択し、選択したプロセスを時分割して実行する。図50 (a) は、メインルーチンで実行される17種類のプロセスを示している。

[0626] メインルーチンで実行される17種類のプロセスとは、CPUが実行するプロセスを選択、管理するプロセス管理プロセスと、電源スイッチをオフした時の初期動作処理を行なうパワーオンプロセスと、電源スイッチをオフした時の終了処理を行なうパワーオフプロセスと、デジタル無線電話モードにおけるGPI(Global User Interface)処理、及び、データ処理(例: 短縮ダイヤルの設定)を行なうデジタル無線電話プロセスと、クレジットカードモードにおけるGUI処理(例: 利用履歴の表示)、及び、データ処理を行なうクレジットカードプロセスと、個人情報管理モードにおけるGUI処理(例: 個人情報表示)、及び、データ処理(例: ユーザ設定情報の設定)を行なう個人情報管理プロセスと、"決済"の処理を行なう決済プロセスと、"キャンセル"の処理を行なうキャンセルプロセスと、"顧客サービスコール"の処理を行なう顧客サービスコールプロセスと、"問い合わせコール"の処理を行なう問い合わせコールプロセスと、データアップロードの処理を行なうデータアップロードプロセスと、強制的データアップロードの処理を行なう強制的データアップロードプロセスと、データバックアップの処理を行なうデータバックアッププロセスと、リモートアクセスの処理を行なうリモートアクセスプロセスと、サービス提供システムとのセッション確立の処理を行なうセッション確立プロセスと、デジタル無線電話通信を制御するデジタル無線電話通信プロセスと、赤外線通信を制御する赤外線通信プロセスとである。

[0627] 各プロセスには、それぞれ、対応するプログラムモジュールがROM1501及びRAM1502の基本プログラムメモリに存在し、CPU1500が、それらのプログラムモジュールを実行することで、それぞれのプロセスが実行される。

[0628] また、各プロセスには、それぞれのプロセスに対応して、プロセスのステータス(状態)を示す情報がRAM1502上のワーク領域21803に存在し、そのプロセスの起動状態("active")または"inactive")と、実行状態("running"または"idle")と、現在の処理ステップとを示す。起動状態における"active"は、そのプロセスがメインルーチンで実行されるプロセスとして起動されていることを示し、"inactive"は、プロセスが起動されていないことを示し、実行状態における"running"は、そのプロセスが実行中であることを示し、"idle"は、一時停止状態であることを示す。

[0629] 特に、デジタル無線電話プロセス、クレジットカードプロセス、個人情報管理プロセスの実行状態は、パーソナル・クレジット端末の動作モードに对应しており、デジタル無線電話プロセスの実行状態が"running"の時、パーソナル・クレジット端末はデジタル無線電話モード、クレジットカードプロセスの実行状態が"running"の時、クレジットカードモード、個人情報管理プロセスの実行状態が"running"の時、個人情報管理モードとなる。デジタル無線電話プロセス、クレジットカードプロセス、個人情報管理プロセスの実行状態は、常に、一つのプロセスだけが"running"を示し、その他は"idle"を示す。以下では、このプロセスのステータスを示す情報を、プロセスステータスと呼ぶ。

[0630] メインルーチンでは、CPU1500は、プロセス管理プロセスと、プロセスリストに登録されているプロセスとを、時分割して繰り返し実行する。プロセスリストは、プロセス管理プロセス以外の起動中のプロセスを示すリストであり、プロセス管理プロセスが、このプロセスリストを更新する。プロセス管理プロセスは、メインルーチンにおいて、常に実行されるプロセスであり、プロセスリストと各プロセスのプロセスステータスとを更新して、メインルーチンで実行するプロセスを選択する。

[0631] プロセス管理プロセスは、メインルーチンの他のプロセス、または前記処理ルーチンの処理から送られるプロセスの生成要求メッセージと、各プロセスのプロセスステータスとに基づいて、プロセスリストを更新する(図50 (b) 参照)。

[0632] 図51は、CPU1500が行なう処理のフローを一、一般化した概念図として表したものである。図50 (b) のように、プロセスリスト22000に、N個 (Nは0以上の整数) のプロセスが登録されている場合の処理のフローを示している。

[0633] 図51において、まず、パーソナル・クレジット端末100をリセットすると、ステップ22100へ進み、CPU1500は、リセット処理を行ない、リセット処理を完了すると、ステップ22101へ進む。リセット処理では、RAM1502上に定義された整數の初期化、及び、内部レジスタの初期化と、プロセス管理プロセスの生成とを伴う。

[0634] ステップ22101では、CPU1500は、プロセス管理プロセスを実行し、プロセスリストと各プロセスのプロセスステータスとを更新して、(N≥1の場合) ステップ22102へ進む (N=0の場合には、ステップ22101へ戻る)。

[0635] (N≥1の場合) ステップ22102では、プロセスリスト22000の1番目に登録されているプロセスのステータスが、"running"か、"idle"かを調べ、"idle"の場合には、(N≥2の場合) ステップ22104へ進む (N=1の場合には、ステップ22101へ戻る)。

[0636] ステップ22103へ進み、1番目のプロセスを実行して、(N≥2の場合) ステップ22104へ進む (N=1の場合には、ステップ22101へ戻る)。

[0637] ステップ22105からステップ22107に相当する処理を繰り返す。但し、ステップ22107からステップ22107に相当する処理の内容は、ステップ22101のプロセス管理プロセスによって変化する。

[0638] 次に、ステップ22111で、interruptのビット28の値から、優先順位が否かを調べ、優先順位でない場合(interrupt(0)1128)=0、ステップ22113へ進み、処理済みの場合(interrupt(0)1128)=1は、ステップ22115へ進み、デジタル無線電話プロセスの生成要求メッセージをプロセス管理プロセスに送って、ステップ22113へ進む。

[0639] ステップ22113で、interruptのビット26の値から、フックデータ割込が否かを調べ、フックデータ割込でない場合(interrupt(0)1130)=0、ステップ22115へ進み、フックデータ割込の場合(interrupt(0)1130)=1は、ステップ22114へ進み、データアップロード処理を行なうセッション確立プロセスの生成要求メッセージをプロセス管理プロセスに送って、ステップ22115へ進む。

(62)

(63)

【06440】 ステップ22115では、Interrupt1のビット25の値から、バックアップ解除が否かを調べ、バックアップ解除でない場合(Interrupt1(b125)=0)、ステップ22117へ進み、バックアップ解除の場合(Interrupt1(b125)=1)は、ステップ22116へ進み、バックアップ解除の生成要求メッセージをプロセス管理プロセスに送って、ステップ22117へ進む。

【06441】 ステップ22117では、Interrupt1のビット24の値から、キー解除が否かを調べ、キー解除でない場合(Interrupt1(b124)=0)、解除処理を終了し、元のメインルーチンの処理へ戻り、キー解除の場合(Interrupt1(b124)=1)は、ステップ22118へ進む。

【06442】 ステップ22118では、Interrupt1の“電源”ビット(b116)の値を調べ、0の場合には、解除処理を終了し、元のメインルーチンの処理へ戻り、1の場合には、電源スイッチが操作されたと判定し、ステップ22119へ進む。

【06443】 ステップ22119では、Interrupt1の“パワー”ビット(b113)の値を調べ、0の場合には、パワーオフの操作が行なわれたと判定し、ステップ22121へ進み、1の場合には、パワーオフの操作が行なわれたと判定し、ステップ22120へ進む。

【06444】 ステップ22120では、パワーオンプロセスの生成要求メッセージをプロセス管理プロセスに送って、解除処理を終了し、元のメインルーチンの処理へ戻る。

【06445】 ステップ22121では、パワーオフプロセスの生成要求メッセージをプロセス管理プロセスに送って、解除処理を終了し、元のメインルーチンの処理へ戻る。

【06446】 解除処理ルーチン22122からメインルーチン22109に戻ってきたCPU1500は、解除処理ルーチンへ戻す直前の処理ステップからメインルーチンの処理を再開する。解除処理ルーチンにおいて、プロセス管理プロセスに送られたプロセスの生成要求メッセージは、解除処理ルーチンからメインルーチンへ戻って、最初に実行するステップ22101のプロセス管理プロセスの処理において評価され、要求されたプロセスが、プロセスリストに登録される。そして、要求されたプロセスは、それ以降のメインルーチンの処理において実行される。

【06447】 例えば、パーソナル・クレジット端末100をリセットした場合、リセットの直後は、プロセスリストには、何も登録されていない。したがって、CPU1600は、リセット処理22100で生成したプロセス管理プロセスをメインルーチンで繰り返す(図52(a)参照)。一方、リセットによって、制御ジョック508は、解除レジスタ(N7)のビット24(キー解除)とビット16(“電源”)とに1を設定して、解除信号1519をアサートする。この時、電源スイッチ209がオン状態の場合には、CPU1500は、この解除による解除処理

ルーチンの処理を経て、メインルーチンにおいてパワーオンプロセスを実行し、電源スイッチ209がオフの状態の場合には、CPU1500は、この解除による解除処理ルーチンの処理を経て、メインルーチンにおいてパワーオフプロセスを実行する。

【06448】 図52(c)は、電源スイッチをオフした場合、または、リセット時に電源スイッチがオフの状態にあった場合の解除処理フローを示している。パワーオフプロセスでは、LCDの表示の消去や、キー操作制御レジスタ(RECT12)1612をアクセスして、電源スイッチ209だけが有効になる設定をするなどの終了処理を行なう。パワーオフプロセスの処理を完了すると、CPU1500は、ホルト状態に移行し、メインルーチンの処理を停止する。CPU1500は、電源スイッチのオン操作による解除、または、アップデート解除、及び、バッテリー補込によってのみ、ホルト状態から通常の動作状態に戻り、解除処理ルーチンの処理の後、メインルーチンの処理を再開する。

【06449】 図52(b)は、電源スイッチをオンした場合、または、リセット時に電源スイッチがオンの状態にあった場合の解除処理フローを示している。パワーオンプロセスでは、LCDの表示の初期化や、RAM1502上に定義された変数と、内部レジスタの設定、及び、デジタル無線電話プロセスと、クレジットカードプロセスと、個人情報管理プロセスの生成要求メッセージをプロセス管理プロセスに送る初期動作処理を行なう。これらのプロセスの生成要求メッセージによって、プロセスリストには、デジタル無線電話プロセスと、クレジットカードプロセス、個人情報管理プロセスと、登録される。メインルーチンにおいて、これらのプロセスが実行される。但し、各プロセスのプロセスステータスの実行状態は保持されているので、パワーオン時の動作モードは、前回、電源スイッチをオフした時の動作モードになる。

【06501】 図53は、パワーオンプロセスの処理の後、または、パーソナル・クレジット端末が、“解除”、“キャンセル”、“顧客サービスコール”、“問い合わせコール”、“データアップデート”、“リモートアクセス”等の処理をしていない定常状態の時のCPUの処理フローを示している。この時、プロセスリストには、デジタル無線電話プロセス、クレジットカードプロセス、個人情報管理プロセスの3つのプロセスが登録されているが、プロセスステータスの実行状態が“running”であるのは1つだけであり、パーソナル・クレジット端末の動作モードは、プロセスステータスの実行状態が“running”を示すプロセスに対応する動作モードにある。

【06511】 ユーザが行なう操作は、解除処理ルーチンの処理によって、解除レジスタ1100の解除要因として、RAM1502上のワードInterrupt1にコピーされ、パーソナル・クレジット端末の動作モードに対応するプ

(64)

ロセス(デジタル無線電話プロセス、または、クレジットカードプロセス、または、個人情報管理プロセス)によって、解釈され、ユーザの操作に対応する処理が行なわれる。そして、支払処理607、キャンセル操作304、問い合わせコール操作1113等の操作をした場合、または、顧客サービスコール1103を受信した場合に、それぞれ、支払プロセス、キャンセルプロセス、問い合わせコール決済プロセス、キャンセルプロセス、問い合わせコールプロセスの生成を要求するメッセージをプロセス管理プロセスに送る。

【0652】 例えば、図54は、“決済”の処理時のCPU1500の処理フローを示している。ユーザが、支払操作を行なうことによって、定常時のプロセス以外に、決済プロセス、セッション確立プロセス、デジタル無線電話プロセス、外部通話プロセスが起動される。

【0653】 次に、クレジット決済端末300の内部の構成を説明する。

【0654】 図55(a)は、クレジット決済端末300のプロック構成図である。

【0655】 クレジット決済端末300は、ROM(Read Only Memory)22501に格納されたプログラムにしたがって、送信データと受信データの処理、及び、バス22529を介して、他の構成要素の制御を行なうCPU(Central Processing Unit)22500と、CPU22500が処理するデータ、及び、CPU22500が処理したデータが格納されるRAM(Random Access Memory)22502、及びハードディスク22503と、クレジット決済端末のターミナルID、電話番号、マーチャントのマーチャントID、サブイベントと公開鍵、及び、サービス提供システムのサービス提供者ID、電話番号(サービス提供システムの電話番号には、サービス提供者の公開鍵が格納されるEEPROM(Electrically Erasable Programmable Read Only Memory)22504と、CPU22500の制御にしたがってLCD302の動作を制御し、CPU22500によって設定された画像をLCDに表示させるLCDコントローラ22505と、CPU22500の制御にしたがってデータの暗号化処理及び復号化処理を行なう暗号処理プロセス22506と、CPU22500の制御にしたがって送信データの暗号化及び受信データの復号化を行なうデータコーデック22507と、

外部線受発光モジュール301と接続するシリアルポート22509と、パラレルデータとシリアルデータとの両方向の変換を行なう直列-並列変換回路22508と、マーチャントによるモジュールスイッチ304、フックスイッチ305、ファンクションスイッチ306、テンキースイッチ307、実行スイッチ308、または電源スイッチ209のスイッチ操作を抽出するキー操作制御部22511と、スピーカ22512と、受話器303のレシーバをドライバし、受話器303のマイクから入力するアナログ音声信号を増幅して音声コーデック22514へ供給する音声処理部22513と、アナログ音声信号22514

4のデジタル音声データへの符号化と、デジタル音声データのアナログ音声信号22514への復号化とを行なう音声コーデック22514と、デジタル音声データとデータ通信データとを多重化した送信データ生成と、多重化された受信データからデジタル音声データとデータ通信データとを抽出するチャネルコーデック22515と、デジタル無線電話回路110との通信アダプタであるデジタル通信アダプタ22516と、キャッシュレジスタ311との間を結ぶRS-232Cケーブル313のインターフェース回路であるRS-232Cインターフェイス22517と、キー操作制御部22513、チャネルコーデック22516、RS-232Cインターフェイス22517から入力する解除信号の処理、及び、CPU22500が、キー操作制御部22513、音声処理部22513、音声コーデック22514、チャネルコーデック22515の内部のレジスタをアクセスする際の、インターフェースの役割を果たす制御ジョック部22510とを備えている。

【0656】 暗号処理プロセス22508は、秘密鍵方式の暗号化、復号化と、公開鍵方式の暗号化、復号化の機能を持ち、CPU22500によって設定された暗号方式と暗号とで、CPU22500によって設定されたデータを、暗号化処理、または、復号化処理する。CPU22500は、この暗号処理プロセス22508の暗号化及び復号化の機能を用いて、メッセージのデジタル署名処理、または、封鎖の復号化処理を行ない、また、封鎖化されたメッセージの暗号化処理を行ない、また、デジタル署名されたメッセージのデジタル署名の検証処理を行なう。

【0657】 データコーデック22507は、CPU22500の制御にしたがって、送信データの暗号化、及び、受信データの復号化を行なう。この場合の暗号化とは、通信制情報、誤り訂正情報を含んだ、実際に送信されるデータを生成する処理を意味し、復号化とは、受信データに対し、誤り訂正処理を施し、余分な通信制情報を取り除き、本来、送り手が送信しようとしたデータを生成する処理を意味する。データコーデック22507は、デジタル無線電話のデータ通信におけるデータの暗号化、復号化と、赤外線通信におけるデータの暗号化、復号化の機能を持ち、CPUに設定されたデータに対して、CPUに設定された暗号化処理、復号化処理を行なう。

【0658】 例えば、デジタル署名処理と封鎖化処理とを施したメッセージを、デジタル無線電話で送信する場合に、CPU22500は、暗号処理プロセス22506を用いて、メッセージのデジタル署名処理と、封鎖化処理とを行ない、さらに、データコーデック22507を用いて、デジタル署名処理と封鎖化処理とを施したメッセージを、デジタル無線電話のデータ通信のデータ形式に符号化して、それを、制御ジョック部22510を介して、チャネルコーデック22515へ送る。

【0659】 逆に、デジタル署名処理と封鎖化処理とが施されたメッセージを、デジタル無線電話で受信した場合、

(65)

合には、C P U 235000は、受信したメッセージを、制御ロジック部23510を介して、チャンネルコーデック23515から読み出し、データコーデック23507を用いて、受信したメッセージを復号化し、さらに、暗号処理プロセス23506を用いて、封装化されているメッセージの暗号の復号化処理とメッセージに施されたデジタル署名の検証処理を行なう。

【0660】同様に、デジタル署名処理と封装化処理とを施したメッセージを、送外線通信で送信する場合に、C P U 23500は、暗号処理プロセス23506を用いて、メッセージのデジタル署名処理と封装化処理とを行ない、さらに、データコーデック23507を用いて、デジタル署名処理と封装化処理とを施したメッセージを、送外線通信のデータ形式で符号化して、それを、直列・並列変換回路2350へ送る。

【0661】逆に、デジタル署名処理と封装化処理が施されたメッセージを、送外線通信で受信した場合には、C P U 23500は、受信したメッセージを、直列・並列変換回路2350から読み出し、データコーデック23507を用いて、受信したメッセージを復号化し、さらに、暗号処理プロセス23506を用いて、封装化されているメッセージの暗号の復号化処理とメッセージに施されたデジタル署名の検証処理を行なう。

【0662】直列・並列変換回路2350と、シリアルポート2309、シリアルケーブル10を介して接続される赤外線受光モジュール301は、図55(b)に示すように、クレンジック技術と他のインターフェイスであるシリリアルポート2355と、直列・並列変換回路から入力するデジタル信号2356を、実際に、送外線として送信される信号に変換、または、受信したアナログ信号2356をシリリアル・デジタル信号23539に変換する変換回路23556と、復変換回路23561によって変換された信号23560を、送外線に変換して発光、または、受光した送外線をアナログ信号23561に変換する赤外線受光部23557とを具備している。

【0663】キー操作制御部23511は、マニピュレータ、モンスイッチ304、フックスイッチ306、フックジョイントスイッチ308、テンキースイッチ307、実行スイッチ308、電源スイッチ309のいずれかのスイッチを押すと、キー操作制御部23511は、C P U 23500に、スイッチ操作に対応する処理を促す割込信号23539をアサートする。また、キー操作制御部23511は、図56に示すように、各スイッチの有効/無効を設定するキー操作制御レジスタ(CTRL)23510を具備している。C P U 23500は、このキー操作制御レジスタ(CTRL)23510をアクセスして、各スイッチの有効/無効を設定する。

【0664】音声処理部23513は、図56に示すように、音声処理動作を制御する音声処理部制御レジスタ(SCR)23505を具備している。C P U 23500は、この音声処理部制御レジスタ(SCR)23505をアクセスして、音声処

理部23513の動作を制御する。例えば、デジタル電話の着呼要求を受信した場合に、C P U 23500は、音声処理部制御レジスタ(SCR)23505にアクセスして、デジタル電話の着呼音を出力する設定を行なう。これによって、音声処理部23513が、スビー23512をドライバとして、デジタル電話の着呼音を出力する。但し、サービスマニュアル102からの着呼要求であった場合には、着呼音は出力せず、C P U 23500は、サービスマニュアルのセリジョンを確立する処理を開始する。

【0665】音声コーデック23514は、音声処理部23513から入力するアナログ音声信号23544のデジタル音声データへの符号化に、チャンネルコーデック23515から読み出したデジタル音声データのデジタル音声信号23543への符号化を行なう。アナログ音声信号23543は、音声処理部23513へ供給され、音声処理部23513が、アナログ音声信号23543を増幅して、受信部2303のレシーバをドライブすることによって、レシーバから音声出力される。符号化によって生成されたデジタル音声データは、チャンネルコーデック23515へ供給され、送信データに変換される。

【0666】また、音声コーデック23514は、音声データの暗号化及び復号化に用いる秘密鍵方式の暗号鍵を格納する音声データ暗号鍵レジスタ(ENPT)23511を具備し、この音声データ暗号鍵レジスタ(ENPT)23511に、C P U 23500によって音声データ暗号鍵が設定された場合、音声コーデック23514は、アナログ音声信号23544のデジタル音声データへの符号化と同時に、デジタル音声データの暗号化を行ない、デジタル音声データのデジタル音声信号23544への符号化と同時に、デジタル音声データの暗号の復号化を行なう。

【0667】チャンネルコーデック23515には、送信するデータとして、二重復のデータが入力される。一つは、音声コーデック23514からデジタル音声信号23547として入力するデジタル音声データであり、もう一つは、C P Uから、制御ロジック部23510を介して、デジタル信号23551として入力するデータ通信データである。

【0668】チャンネルコーデック23515は、デジタル音声データ及びデータ通信データの識別情報、ヘッダ情報として、それぞれのデータに付加し、このデジタル音声データとデータ通信データとを多重化したデジタル信号23548をデジタル通信アダプタ23516へ供給する。

【0669】その逆に、チャンネルコーデック23515は、デジタル通信アダプタ23516から入力するデジタル信号23548に対して、まず、タミナルIDを照合し、次に、データのヘッダ情報から、デジタル音声データかデータ通信データかを識別し、それぞれ、デジタル音声信号23547及びデジタル信号23551として、音声コーデック23511と制御ロジック部23510とへ供給する。また、チャンネルコーデック23515は、デジタル電話を着信した時と、データ通信データを受信した時とに、割込信号22

548をアサートし、デジタル音声データを受信した時に、制御信号23548をローレベルにする。割込信号23548は、C P U 23500に、デジタル電話の着信時の処理と、データ通信データの処理とを促す割込信号であり、制御信号23545は、音声コーデック23514に、受信したデジタル音声データの処理を促すローグライアの制御信号である。

【0670】チャンネルコーデック23515は、こうした動作を行なうために、図56に示すように、タミナルIDを格納するIDレジスタ(ID)23503と、チャンネルコーデック23515の動作を制御するチャンネルコーデック制御レジスタ(CTRL)23504と、音声コーデック23514から入力されるデジタル音声データを格納する音声送信バッファ23505と、受信データの途中から抽出したデータ通信データと、受信データの途中から抽出したデータ通信データを格納するデータ受信バッファ23508とを具備している。

【0671】制御信号23545は、チャンネルコーデック23515に、音声送信バッファ23505と音声受信バッファ23506への、音声コーデック23514による書き込みと読み出しの動作を示す制御信号であり、音声コーデック23514は、制御信号23546をローレベルにして、音声送信バッファ23505にデジタル音声データを書き込み、制御信号23546をハイレベルにして、音声受信バッファ23506からデジタル音声データを読み出す。

【0672】制御信号23550は、チャンネルコーデック23515に、データ送信バッファ23507とデータ受信バッファ23508への、制御信号23551を介したC P U 23500による書き込みと読み出しの動作を示す制御信号であり、制御信号23550をローレベルにして、データ送信バッファ23507にデータ通信データを書き込み、制御信号23550をハイレベルにして、データ受信バッファ23508からデータ通信データを読み出す。

【0673】デジタル通信アダプタ23516は、デジタル信号23548をデジタル電話通信のフォーマットにエンコードしてデジタル電話通信回路110に出力する。逆に、デジタル通信アダプタ23516は、デジタル電話通信回路110から受信した信号をデコードして、デジタル信号23548をチャンネルコーデック23515に供給する。

【0674】R S - 2 3 2 C インターフェイス23517は、R S - 2 3 2 C ケーブル13を接続するインターフェイス回路であり、クレンジック技術では、このR S - 2 3 2 C インターフェイス23517を介して、キャプティブレジスタ311と通信する。R S - 2 3 2 C インターフェイス23517は、キャプティブレジスタ311からデータを受信すると、割込信号23552をアサートする。割込信号23552は、C P U 23500に、R S - 2 3 2 C インターフェイス23517を介した、キャプティブレジスタ311とのデータ通信の処理を

(66)

促す割込信号である。

【0675】また、制御ロジック部23510は、図56に示すように、その内部に、クロックカウンタ(CLOCK)22600、アツタデータ時刻レジスタ(OUTIME)22601、割込レジスタ(INIT)22602の3つのレジスタを内蔵する。

【0676】クロックカウンタは、現在の時刻をカウンタするカウンタ。アツタデータ時刻レジスタは、クレンジック技術端末300が、サービスマニュアルと通信して、R A M 22502及びハードバス23503上のデータを更新する処理(データアツタデータ処理)を行なう時刻を格納するレジスタ。割込レジスタは、C P U 23500への割込の要因を示すレジスタである。

【0677】制御ロジック部23510は、クロックカウンタ22600の値がアツタデータ時刻レジスタ23503の値に一致した場合、割込信号23559、23548、23550のいずれかの割込信号がアサートされた場合に、その割込要因を割込レジスタ(INIT)22602に設定して割込信号23518をアサートし、C P Uに割込処理を促す。C P U 23500は、割込処理で、割込レジスタを読みだし、その割込要因に応じた処理を行なう。

【0678】この割込レジスタ(INIT)の各ビットフィールドは、図57(a)に示すように意味づけられている。この意味づけは、第1の実施形態において、図27(b)を用いて説明したものと同一である。

【0679】次に、R A M 22501に格納されるデータに関して説明する。

【0680】図58は、R A M 22501に格納されるデータのR A M アドレスの模式図である。

【0681】R A M 22501には、基本プログラム領域22800、サービスマニデータ領域22801、マニデータ領域22802、マニデータ領域22803、及びマニデータ領域22804の5つの領域がある。基本プログラム領域22800は、R O M 22501に格納されているプログラムのバージョンアップされたモジュール、及び、バッチプログラムや追加プログラムが格納される。マニデータ領域22802は、マニデータが自由に使用できる領域。マニデータ領域22803は、C P U 100がプログラムを実行する際に使用する作業領域、マニデータ領域22804は、クレンジック技術が受信した情報を一時的に格納する領域である。

【0682】サービスマニデータ領域22801は、マニデータ・マニデータ・マニデータ・マニデータのID情報や、取扱いマニデータ情報、履歴情報を格納する領域であり、この領域のデータは、サービスマニシステムに管理される。サービスマニデータ領域22801には、さらに、マニデータ管理情報22805、マニデータ管理情報22806、マニデータ管理情報22807、電話情報22808、クレンジックカードID管理情報22809、販売履歴リスト22810の6つの領域がある。

【0683】マニデータ管理情報22805は、サービスマニデータ領域22801に格納されている情報の管理情報を格納する領域。マニデータ管理情報22806は、マニデータの各

称、サービス提供者との契約内容等の情報を格納する領域、マーチャント設定情報22807は、パーソナル・リモート・クレジット決済サービスに関する、マーチャントの固定情報を格納する領域、電話情報22808は、デジタル電話に関連する情報を格納する領域、クレジットカードリスト22809は、マーチャントが取り扱うことができるクレジットカードのリスト情報、クレジットカードのリスト情報を格納する領域、販売履歴リスト22810は、パーソナル・リモート・クレジット決済サービスでの販売履歴情報を格納する領域である。

〔0 6 8 4〕次に、サービスデータ領域22801に格納される情報について詳しく説明する。

〔0 6 8 5〕図5 9は、サービスデータ領域22801に格納される情報の関係を詳細に表した模式図である。

〔0 6 8 6〕データ管理情報22805は、アップデート日時22900、次回アップデート日時22901、ターミナル・システム設定情報22902、マーチャント情報22903、マーチャント設定情報22904、電話情報22905、販売履歴リスト22906、クレジット・アドレス22907の8つの情報によって構成される。

〔0 6 8 7〕アップデート日時22900は、サービス提供システム102が、前回、RAM22502、及び、ハードディスク22503のデータを更新した日時を示し、次回アップデート日時22901は、次回サービス提供システム102によるサービスデータ領域22801のデータの更新の予定日を示す。クレジット決済端末は、次回アップデート日時22901の更新された時間になると、自動的に、データアップデート処理を開始する。

〔0 6 8 8〕この次回アップデート日時22901の値は、アップデート時刻レジスタ21603に設定され、次回アップデート日時22901の時刻になると、クレジット決済端末300は、データアップデート処理を開始する。データアップデート処理は、サービス提供システム102が、RAM、及び、ハードディスクのデータを更新する処理であり、通常、通信のトラフィックが、比較的、少ない時間帯（例：深夜）に、毎日、行なう。

〔0 6 8 9〕ターミナル・システム22902は、クレジット決済端末の状態を示し、マーチャント情報22903、電話情報22905、クレジットカードリスト・アドレス22906、販売履歴リスト・アドレス22907は、それぞれ、マーチャント情報22806、マーチャント設定情報22807、電話情報22808、クレジットカードリスト22809、利用履歴リスト22810が格納されている領域の先頭番地を示す。

〔0 6 9 0〕電話情報22808は、さらに、発信電話番号22908、電話機アドレス22909、短縮ダイヤル設定フィールド・アドレス22910の3つの情報によって構成される。発信電話番号22908は、マーチャントが、前回、かけた電話の電話番号を示し、この情報は、デジタル無線電話

の再送時に用いられる。電話機アドレス22909と、短縮ダイヤル設定フィールド・アドレス22910とは、それぞれ、電話機情報、短縮ダイヤル設定フィールドが格納されているハードディスク22503上のアドレスを示す。

〔0 6 9 1〕クレジットカードリスト22809は、マーチャントが取り扱うことができるクレジットカードのリスト情報が格納されている。クレジットカードリスト22809では、一つのクレジットカードに対して、クレジットカード名22911(22913、22915)、サービスコード・リスト・アドレス22912(22914、22916)の2つの情報が格納されている。クレジットカード名22911(22913、22915)は、マーチャントが取り扱うことができるクレジットカードの名前を示し、サービスコード・リスト・アドレス22912(22914、22916)は、そのクレジットカードによって提供されるサービスの内、マーチャントが取り扱うことができるサービスの種類を示すサービスコード・リストが格納されているハードディスク22503上のアドレスを示す。サービスコード・リストは、マーチャントが取り扱うことができるサービスコードと、支払オプションコードとのリストである。

〔0 6 9 2〕販売履歴リスト22810は、パーソナル・リモート・クレジット決済サービスでの販売履歴情報を格納する領域である。販売履歴リスト22810では、一つのパーソナル・リモート・クレジット決済サービスの販売に対して、トランザクション番号22917(22921)、サービスコード22918(22922)、販売時刻22919(22923)、販売情報22920(22924)の4つの情報が格納される。

〔0 6 9 3〕トランザクション番号22917(22921)は、ユーザとの取引をユニークに示す番号であり、支払オプション・広告609を生成する際に、クレジット決済端末が実行する番号、サービスコード22918(22922)は、ユーザが利用したクレジットカードサービスの種類を示すコード番号、販売時刻22919(22923)は、パーソナル・リモート・クレジット決済サービスで販売した時刻、販売情報22920(22924)は、決済完了通知が格納されているアドレスを示す。

〔0 6 9 4〕販売情報アドレス22920(22924)には、ハードディスク22503上のアドレスを示すリモート・アドレス、または、サービスの提供システム102のマーチャント情報サーバ103上のアドレスを示すリモート・アドレスが格納される。販売情報アドレス22920(22924)に、リモート・アドレスが格納されている場合、マーチャントが、その販売履歴情報をアクセスすると、クレジット決済端末は、サービス提供システムから、販売情報をテンポラリ領域にダウンロードして、LCDに表示する。

〔0 6 9 5〕販売情報アドレス22920(22924)に格納されるアドレスは、サービス提供システム102によって決定される。データアップデート処理の際に、各販売情報の販売時刻と比較し、販売時刻が最近の販売情報に、ローカルアドレスが割り当てられる。但し、ハードディスク2250

3の容量に余裕がある場合には、全ての販売情報アドレスが、ローカルアドレスである場合もある。

〔0 6 9 6〕次に、CPU22500が行なう処理について説明する。

〔0 6 9 7〕図6 1は、CPU22500が行なう処理フローの概念図である。

〔0 6 9 8〕図6 1に示すように、CPU22500が行なう処理には、メインルーチン23109と、割込処理ルーチン23122との2つの処理ルーチンがある。メインルーチンは、送信データと受信データとの処理、及び、他の構成要素の制御を行なう処理ルーチンであり、割込処理ルーチンは、外部割込によって要求されるプロセス(処理)を抽出する処理ルーチンである。したがって、CPU22500は、通常、メインルーチンの処理を行なう。割込発生22516がアサートされると、CPU22500は、メインルーチンから割込処理ルーチンへ飛び、割込処理を行ない、割込処理を終了すると、メインルーチンに戻り、元のメインルーチンの処理を再開する。

〔0 6 9 9〕CPU22500が、メインルーチンの中で実行するプロセスは、17種類のプロセスであり、CPU22500は、プロセスを動的に選択し、選択したプロセスを時分割して実行する。図6 0 (a) は、メインルーチンで実行される17種類のプロセスを示している。

〔0 7 0 0〕メインルーチンで実行される17種類のプロセスとは、CPUが実行するプロセスを選択、管理するプロセス管理プロセスと、電話スイッチをオンした時の初期動作処理を行なうパワーオンプロセスと、電話スイッチをオフした時の終了処理を行なうパワーオフプロセスと、デジタル電話モードにおけるGUI(Graphical User Interface)処理、及び、データ処理（例：短縮ダイヤルの設定）を行なうデジタル電話プロセスと、クレジット決済モードにおけるGUI処理（例：販売履歴表示）、及び、データ処理を行なうクレジット決済プロセスと、マーチャント情報管理モードにおけるGUI処理（例：マーチャント情報の表示）、及び、データ処理（例：マーチャント情報の更新）を行なうマーチャント情報管理プロセスと、“決済”の処理を行なう決済プロセスと、“顧客サービスコール”の処理を行なう顧客サービスコールプロセスと、リモートアクセスの処理を行なうリモートアクセスプロセスと、サービス提供システムとのセッション確立の処理を行なうセッション確立プロセスと、デジタル電話通信を制御するデジタル電話通信プロセスと、赤外線通信を制御する赤外線通信プロセスと、RS-232Cインターフェースを介したデータ通信を制御する外端インターフェース通信プロセス

とである。  
〔0 7 0 1〕各プロセスには、それぞれ、対応するプログラムモジュールが、ROM22501、及び、RAM22502の基本プログラム領域21803に存在し、CPU22500が、それらのプログラムモジュールを実行することで、それぞれのプロセスが実行される。

〔0 7 0 2〕また、各プロセスには、それぞれのプロセスに対応して、プロセスのステータス（状態）を示す情報がRAM22502上のワーク領域2503に存在し、そのプロセスの起動状態(“active”または“inactive”)と、現在の処理実行状態(“running”または“idle”)と、現在の処理ステータスとを示す。起動状態における“active”は、プロセスが起動されていることを示し、“inactive”は、プロセスが起動されていないことを示し、実行状態における“running”は、そのプロセスが実行中であることを示し、“idle”は、一時停止状態であることを示す。

〔0 7 0 3〕特に、デジタル電話プロセス、クレジット決済プロセス、マーチャント情報管理プロセスの実行状態は、クレジット決済端末の動作モードに対応しており、デジタル電話プロセスの実行状態が“running”の時、クレジット決済端末はデジタル電話モード、クレジット決済プロセスの実行状態が“running”の時、クレジット決済モード、マーチャント情報管理プロセスの実行状態が“running”の時、マーチャント情報管理モードとなる。デジタル電話プロセス、クレジット決済プロセス、マーチャント情報管理プロセスの実行状態は、一つのプロセスだけが“running”を示し、その他は“idle”を示す。以下では、このプロセスのステータスを示す情報を、プロセスステータスと呼ぶ。

〔0 7 0 4〕メインルーチンでは、CPU22500は、プロセス管理プロセスと、プロセスリストに登録されているプロセスを、時分割して繰り返し実行する。プロセスリストは、プロセス管理プロセス以外の起動中のプロセスを示すリストであり、プロセス管理プロセスが、このプロセスリストを更新する。プロセス管理プロセスは、メインルーチンにおいて、常に実行されるプロセスであり、プロセスリストと各プロセスのプロセスステータスとを更新して、メインルーチンで実行するプロセスを選択する。

〔0 7 0 5〕プロセス管理プロセスは、メインルーチンの他のプロセス、または割込処理ルーチンの処理から送られるプロセスの生成要求メッセージと、各プロセスのプロセスステータスとに基づいて、プロセスリストを更新する（図6 0 (b) 参照）。

〔0 7 0 6〕図6 1は、CPU22500が行なう処理のフローを、一般化した概念図として表したものである。図6 0 (b) のように、プロセスリスト23000にN個（Nは0以上の整数）のプロセスが登録されている場合の処理のフローを示している。



【0707】図61において、まず、クロック供給増大300をリセットすると、ステッ73100へ進み、CPU 32500は、リセット処理を行ない、リセット処理を完了すると、ステッ73101へ進み、リセット処理では、RAM2302上に定義された変数の初期化、及び、内部レジスタの初期化、プロセス管理プロセスの生成とを行なう。

【0708】ステッ73101では、CPU32500は、プロセス管理プロセスを実行し、プロセスリストと各プロセスのプロセスタイタスとを更新して、(N≧1の場合) ステッ73102へ進み (N=0の場合には、ステッ73101へ戻る)。

【0709】(N≧1の場合) ステッ73102では、プロセスリスト23000の1番目に登録されているプロセスのステイタスが、"running"か、"idle"かを調べ、"idle"の場合には、(N≧2の場合) ステッ73104へ進み (N=1の場合には、ステッ73103へ戻る)、"running"の場合には、ステッ73103へ進み、1番目のプロセスを実行して、(N≧2の場合) ステッ73104へ進み (N=1の場合には、ステッ73101へ戻る)。

【0710】(N≧2の場合) ステッ73104以降は、プロセスリストの1番目のプロセスに対する処理 (ステッ73104、ステッ73103)と同様の手順で、プロセスリストの2番目からN番目のプロセスに対する処理を実行する。CPU32500は、N番目のプロセスに対する処理 (ステッ73106、ステッ73107)を終了すると、ステッ73101へ戻る。つまり、CPU32500は、ステッ73101と、ステッ73104からステッ73107に相当する処理を繰り返す。但し、ステッ73102からステッ73107に相当する処理の内容は、ステッ73101のプロセス管理プロセスによって変化する。

【0711】メインルーチン73109の処理の実行中に、割込信号22518がアサートされると、CPU32500は、割込ルーチン73122へ飛び、割込処理ルーチン73122では、まず、CPU32500は、ステッ73110で、割込レジスタ (INT)を読みだし、RAM (ワーキング領域)上のワーking errorにコピーする。この時、CPUに読みだされた割込レジスタ (INT)は、エコーリセットされ、割込信号22518もリセットされる。

【0712】次に、ステッ73111で、interruptのビット28の値から、割込理由が否かを調べ、割込でない場合 (interrupt (0)128)=0)、ステッ73113へ進み、割込 (interrupt (0)128)=1)は、ステッ73111へ進み、デジタル電話プロセスの生成要求メッセージをプロセス管理プロセスに送って、ステッ73113へ進む。

【0713】ステッ73113では、interruptのビット26の値から、アプデイト割込が否かを調べ、アプデイト割込でない場合 (interrupt (0)128)=0)、ステッ73115へ進み、アプデイト割込の場合 (interrupt (0)128)

=1)は、ステッ73114へ進み、データアプデイトプロセスの生成要求メッセージをプロセス管理プロセスに送って、ステッ73115へ進む。

【0714】ステッ73115では、interruptのビット25の値から、外部1F割込が否かを調べ、外部1F割込でない場合 (interrupt (0)125)=0)、ステッ73117へ進み、外部1F割込の場合 (interrupt (0)125)=1)は、ステッ73118へ進み、外部1F通信プロセスの生成要求メッセージをプロセス管理プロセスに送って、ステッ73117へ進む。

【0715】ステッ73117では、interruptのビット24の値から、キー割込が否かを調べ、キー割込でない場合 (interrupt (0)124)=0)、割込処理を終了し、元のメインルーチンの処理へ戻り、キー割込の場合 (interrupt (0)124)=1)は、ステッ73118へ進む。

【0716】ステッ73118では、interruptの"電線"ビット (0)116)の値を調べ、0の場合には、割込処理を終了し、元のメインルーチンの処理へ戻り、1の場合には、電線入イッチが操作されたと判定し、ステッ73119へ進む。

【0717】ステッ73119では、interruptの"パワー"表示ビット (0)131)の値を調べ、0の場合には、パワーオンの操作が行われたと判定し、ステッ73121へ進み、1の場合には、パワーオンの操作が行われたと判定し、ステッ73120へ進む。

【0718】ステッ73120では、パワーオンプロセスの生成要求メッセージをプロセス管理プロセスに送って、割込処理を終了し、元のメインルーチンの処理へ戻る。

【0719】ステッ73121では、パワーオンプロセスの生成要求メッセージをプロセス管理プロセスに送って、割込処理を終了し、元のメインルーチンの処理へ戻る。

【0720】割込処理ルーチン73122からメインルーチン73109に戻ってきたCPU32500は、割込処理ルーチンへ飛ぶ直前の処理ステッ73109からメインルーチンの処理を再開する。割込処理ルーチンにおいて、プロセス管理プロセスに送られたプロセスの生成要求メッセージは、割込処理ルーチンからメインルーチンへ戻って、最初に実行するステッ73101のプロセス管理プロセスの処理において評価され、要求されたプロセスが、プロセスリストに登録される。そして、要求されたプロセスは、それ以降のメインルーチンの処理において実行される。

【0721】例えば、クロック供給増大300をリセットした場合、リセットの直後は、プロセスリストには何も登録されていないため、CPU32500は、リセット処理33000の生成したプロセス管理プロセスをメインルーチンで繰り返す (図52 (a)参照)。一方、リセットによって、例題クロック部23010は、割込レジスタ (INT)のビット24 (キー割込)とビット16

("電線")とに1を設定して、割込信号22518をアサートする。この時、電線入イッチ309が0の状態の場合には、CPU32500は、この割込による割込処理ルーチンの処理を終了、メインルーチンにおいてパワーオンプロセスを実行し、電線入イッチ309が0の状態の場合には、CPU32500は、この割込による割込処理ルーチンの処理を終了、メインルーチンにおいてパワーオンプロセスを実行する。

【0722】図52 (c)は、電線入イッチをオンした場合、または、リセット時に電線入イッチがオンの状態にあつた場合の処理フローを示している。パワーオンプロセスでは、LCDの表示の消去や、キー操作制御レジスタ (DECT) 33810をアクセスして、電線入イッチ309だけが有効になる設定をするなどの終了処理を行なう。パワーオンプロセスの処理を完了すると、CPU32500は、ホルト状態に移行し、メインルーチンの動作を停止する。CPU32500は、電線入イッチのオン操作による割込、または、アプデイト割込によってのみ、ホルト状態から通常の動作状態に戻り、割込処理ルーチンの処理の後、メインルーチンの処理を再開する。

【0723】図52 (b)は、電線入イッチをオンした場合、または、リセット時に電線入イッチがオンの状態にあつた場合の処理フローを示している。パワーオンプロセスでは、LCDの表示の初期化や、RAM23502上に定義された変数と、内部レジスタの設定、及び、デジタル電話プロセスと、クロック供給プロセス、ワーキングメモリ管理プロセスとの生成要求メッセージをプロセス管理プロセスに送る初期動作処理を行なう。これらのプロセスの生成要求メッセージは、プロセスリストには、デジタル電話プロセスと、クロック供給プロセス、ワーキングメモリ管理プロセスとが登録され、メインルーチンにおいて、これらのプロセスが実行される。但し、各プロセスのプロセスタイタスの実行状態は保存されているので、パワーオン時の動作モードには、前回、電線入イッチをオンした時の動作モードになる。

【0724】図62は、パワーオンプロセスの処理の終了後、または、クロック供給増大が、"故障"、"キヤンセル"、"顧客サービスコール"、"問い合わせコール"、"データアプデイト"、"リモートアクセス"等の処理をしていない定常状態の時のCPUの処理フローを示している。この時、プロセスリストには、デジタル電話プロセス、クロック供給プロセス、ワーキングメモリ管理プロセスの3つのプロセスが登録されているが、プロセスタイタスの実行状態が"running"であるのは1つだけであり、クロック供給増大の動作モードは、プロセスタイタスの実行状態が"running"を示すプロセスに対応する動作モードにある。

【0725】ワーキングが行なうキー操作は、割込処理ルーチンの処理によって、割込レジスタ22503の割込

要因として、RAM23502上のワーking interruptにコピーされ、クロック供給増大の動作モードに対応するプロセス (デジタル電話プロセス、または、クロック供給プロセス、または、ワーキングメモリ管理プロセス)によって、解釈され、ワーキングの動作に対応する処理が行なわれる。そして、クロック供給の動作604、キヤンセル動作901、顧客サービスコール動作1200等の操作をした場合、または、問い合わせコール1116を受信した場合に、それぞれ、故障プロセス、キヤンセルプロセス、顧客サービスコールプロセス、問い合わせコールプロセス等の対応するプロセスの生成を要求するメッセージをプロセス管理プロセスに送る。

【0726】例えば、図63は、"故障"の処理時のCPU32500の処理フローを示している。ワーキングが、クロック供給の操作を行なうことによって、定常時のプロセス以外に、故障プロセス、メンテナンスプロセス、デジタル電話通信プロセス、外部通信プロセスが起動される。

【0727】次に、デジタル署名処理及び封書化処理について説明する。パーソナル、クロック増大101、クロック供給増大とサービス提供システムとに送信するメッセージを生成するときや、クロック供給増大がパーソナル、クロック供給増大とサービス提供システムとに送信するメッセージを生成するときなどにデジタル署名処理と封書化処理とが行なわれ、このデジタル署名処理の手順を図64 (a)、(b)に示し、封書化処理の手順を図65 (a)、(b)に示している。また、封書化されたメッセージの復号化処理の手順を図66 (a)、(b)に示し、デジタル署名がされたメッセージのデジタル署名の検証手順を図67 (a)、(b)に示している。これらの手順は、第1の実施形態において、図20、図21、図22及び図23を用いて説明した手順と実質的に同じである。

【0728】次に、サービス提供システム102における処理について説明する。

【0729】サービス提供システム102は、パーソナル、クロック増大100、クロック供給増大101、故障プロセス103と、それぞれ通信を行ない、ユーザ、ワーキング、故障処理機関の三者間の仲介をして、ユーザ、及び、ワーキングに対して、パーソナル・リモート・クロック供給サービスを提供するシステムである。

【0730】図68は、サービス提供システム102における処理のアーキテクチャを示している。

【0731】サービス提供システム102は、パーソナル・リモート・クロック供給サービス (User Process) 23502、ワーキングプロセス (WP: Working Process) 23503、故障処理機関プロセス (TP: Transaction Process) 23504、サービス・チャイナプロセス (SP: Service Director Process) 23501、及び、サービス・

ネーチャプロセス(SMP:Service Manager Process)23800の5種類のプロセスの連携処理によって提供する。図68において、ユーザプロセス23800は、パーソナル・クレジット端末100と1対1に対応して、サービス提供システム102とパーソナル・クレジット端末100との通信のインターフェイスとなるプロセスであり、また、マーチャントプロセス23803は、クレジット決済端末300と1対1に対応して、サービス提供システム102とクレジット決済端末300との通信のインターフェイスとなるプロセス、決済処理機関プロセス23804は、決済システム103に対応して、サービス提供システム102と決済システム103との通信のインターフェイスとなるプロセス、サービス・ディレクタプロセス23801は、ユーザプロセス23802、マーチャントプロセス23803、決済処理機関プロセス23804とそれぞれ通信をして、パーソナル・リモート・クレジット決済サービスを提供するプロセス、サービス・マネージャプロセス23800は、サービス提供システム102上のユーザプロセス、マーチャントプロセス、決済処理機関プロセス、サービス・ディレクタプロセスを管理するプロセスである。「パーソナル・リモート・クレジット決済サービスを提供する」という表現の意味については、後で詳しく説明する。

【0732】図69、図70に、この5種類のプロセスの一覧を示す。

【0733】 サービス提供システム01は、同時に、複数のバーナナル・クレジット端末、及び、複数のクレジット決済端末と通信する場合があり、また、同時に、複数のバーナナル・リモート・クレジット決済サービスと通信を行なう場合や、同時に、複数の決済システムと通信をして、複数のバーナナル・リモート・クレジット決済サービスの処理を行なう場合がある。したがって、ユーザプロセス、マーチャントプロセス、決済処理機関プロセス、及びサービス・ディレクタプロセスは、それぞれ、複数のプロセスが、同時にサービスサーバ100上に存在する場合がある。これらのユーザプロセス、マーチャントプロセス、決済処理機関プロセス、及びサービス・ディレクタプロセスは、サービス・マネージャ・プロセスによって、生成、及び、消去され、管理される。

【0734】また、サービスサーバ000が複製台のコンピュータによって構成される場合には、ユーザプロセス、マージャントプロセス、及び処理制御プロセス、及びサービス・ディレクタプロセスは、各プロセスの処理の負荷が分散されるように、複製台のコンピュータに分散して生成される。

【0735】また、連鎖処理をして、1つのパーソナル・リモート・クレジット決済サービスを提供するプロセスの集合は、サー・ビス・マネージャプロセスによって決定され、そのプロセスの集合は、ユーザプロセス、マーチャントプロセス、決済処理機関プロセスの内1つ以上

のプロセスと、1つのサービス・ディレクタプロセスとによって構成される。以下では、この連携処理を行うようなプロセスの集合をプロセスグループと呼ぶ。  
〔0736〕まず、ユーザプロセス23803について説明する。

【0737】ユーザプロセスは、パーソナル・クレジット端末100との通信制御と、ユーザの認証、パーソナル・クレジット端末100への送信データの暗号化、パーソナル・クレジット端末100からの受信データの復号化、パーソナル・クレジット端末100からの受信データの有効性のチェック、さらに、パーソナル・クレジット端末100との間で、リモートアクセスと、データアップデー、データバックアップの処理を行なうプロセスである。

【0738】ユーザプロセス33003は、サービス提供システム102がパーソナル・クレジット端末100と通信をする場合に、サービス・マネージャプロセス33000によって生成されるプロセスである。サービス・マネージャプロセス33000は、サービス提供システム102と通信する1台のパーソナル・クレジット端末100に対して、1つのユーザプロセス33003を生成する。この時、サービス・マネージャプロセス33000は、サービスサーバ400を構成するコンピュータのメモリ、または、ハードディスク上に、図75の(a)に示すユーザプロセス管理情報4400を生成して、生成したユーザプロセス33003を管理する。

【0739】ユーザプロセス3809には、ユーザプロセス管理情報400と、ユーザ情報サーバ402によって管理されているパーソナル・クレジット端末100の所有者（ユーザ）の属性情報とパーソナル・クレジット端末100（のRAM1502）の逆々にアクセスするパーミッショングが与えられる。逆に、ユーザプロセス3809は、その他の情報にアクセスすることはできない。

【0740】 パーソナル・クレジット燭米100とユーザ  
プロセス3802とは、1対1に対応し、ユーザプロセス  
3802は、パーソナル・クレジット燭米100に対してのみ  
有効なプロセスであり、その他のパーソナル・クレジッ  
ト燭米と、直接、関係することはできない。

【0741】ユーザプロセス33002とパーソナル・クレ  
ジット端末100は、図69の23901と23902の欄に示すメ  
ッセージを用いて通信する。23901の欄のメッセージ  
(リモートAから読取、暗証テストC、暗証テストD応  
答、リモートAアクセス要求、データアップロード要求、  
アップロードデータ、支払要求、キャンセル要求、着信  
応答、問い合わせコール要求、タイムアウト・エラーメ  
ッセージ、セッション・エラーメッセージ)は、パーソ  
ナル・クレジット端末からユーザプロセスに送られるメ  
ッセージを、23901の欄のメッセージ(暗証テストA、  
暗証テストB応答、暗証テストC応答、リモートアクセ  
スデータ、データアップロード応答、アップロードデー

タ、データアップデート命令、機能停止命令、収収着、キャンセル処理収収着、顧客サービスコール、問い合わせコール応答、呼び出し応答、タイムアウト・エラーメッセージ、セッション・エラーメッセージ、タイムアウト・メッセージは、ユーザプロセスからパーソナル・クレジット端末に送られるメッセージを示している。これは他のメッセージを送っても、お互いに、有効なメッセージとして解釈されない。

【0742】また、ユーザプロセス33902は、同一のプロセスグループに属するサービス・ディレクタプロセス33801と、図6の23903と33904の間に示すメッセージをインターフェイスとして通信する。23903の欄のメッセージ(領収書、キャンセル処理領収書、顧客サービスコール、問い合わせコール応答、呼び出し応答、タイムアウト・エラーメッセージ、セッション・エラーメッセージ)は、サービス・ディレクタプロセスからユーザプロセスに送られるメッセージを、23904の欄のメッセージ(支払要求、キャンセル要求、着信応答、問い合わせコール要求、タイムアウト・エラーメッセージ、セッション・エラーメッセージ、タイムアウト・メッセージ)は、ユーザプロセスからサービス・ディレクタプロセスに送られるメッセージを示している。これ以外のメッセージを送っても、お互いに、有効なメッセージとして解読されない。

【0743】さらに、ユーザプロセス338071は、サービス・マネージャプロセス33800と、図69の233906の欄に示すメッセージをインターフェイスとして適応する。233906の欄のメッセージ（支払要求、キャンセル要求、問い合わせ要求、自身のプロセスを消去要求）は、ユーザプロセスからサービス・マネージャプロセスに送られるメッセージを示している。また、図69の233905の欄（ユーザプロセス生成、ユーザプロセス消去）は、サービス・マネージャプロセスのユーザプロセスへの作用を示しており、サービス・マネージャプロセスが、ユーザプロセスの生成と消去を行なう。メッセージの内容については、後で詳しく説明する。

【0744】ユーザプロセスと他のユーザのユーザプロセスとの間の通信のインタラフェイスはなく、ユーザプロセスは、他のユーザプロセスと、直接、通信することはできない。同様に、ユーザプロセスとマーチャントプロセス、ユーザプロセスと決済処理機間プロセス、ユーザプロセスと異なるプロセスグループのサービスディレクタプロセスとの間の通信のインタラフェイスはなく、ユーザプロセスは、マーチャントプロセス、決済処理機間プロセス、及び異なるプロセスグループのサービスディレクタプロセスと、直接、通信することはできない。

【0745】また、ユーザが居住しているサービエリア以外のサービエリアで、パーソナル・クレジット端末を使用する場合には、ユーザが居住するサービエリア

アのサービス提供システム上と、パーソナル・クレジッ  
ト端末を使用するサービスエリアのサービス提供システ  
ム上に、ユーザプロセスが生成される場合がある。この  
ような場合については、後で詳しく説明する。

【0746】次に、マーチャントプロセス23803について説明する。

【0747】マーチャントプロセスは、クレジットカード決済端末300との通信制御と、マーチャントの図証、クレジット決済端末300への送信データの暗号化、クレジット決済端末300からの受信データの復号化、クレジット決済端末300からの受信データの有効性のチェック、さらに、クレジット決済端末300との間で、リモートアクセスと、データアップデータの処理とを行なうプロセスである。

【0748】 マーチャントプロセス238003は、サービス提供システム102がクレジット決済端末300と通信をする場合に、サービス、マネージャプロセス238001によって生成されるプロセスである。サービス・マネージャプロセス238001は、サービス提供システム102と通信する1台のクレジット決済端末300に対して、1つのマーチャントプロセス238003を生成する。この時、サービス・マネージャプロセス238001は、サービスサーバ400を構成するコンピュータのメモリ、または、ハードディスク上に、図75の(b)に示すマーチャントプロセス管理情報4401を生成して、生成したマーチャントプロセス238003を管理する。

【0749】マーチャントプロセス3803には、マーチャントプロセス管理情報401と、マーチャント情報サーバ403によって管理されているクレジット決済端末300の所有者（マーチャント）の属性情報と、クレジット決済端末300のRAM2502及びハードディスク2503のデータにアクセスするパーミッションが与えられ、逆々に、マーチャントプロセス3803は、その他の情報にアクセスすることはできない。

【0750】クレジット決済端末300とマーチャントプロセス23003とは、1対1に対応し、マーチャントプロセス23003は、対応するクレジット決済端末300に対してのみ有効なプロセスであり、その他のクレジット決済端末と、直接、通信することはできない。

【0751】 マーチャントプロセス33003とクレジット決済端末300とは、図69の23507及び23508の欄に示すメッセージを用いて通信する。23507の欄のメッセージ（認証テストA）は、認証テストC、認証テストD（答、リモートアクセス要求、データアップデータ要求、アップロードデータ、信用照会要求、決済要求、領収書、キャンセル要求、増信応答、顧客サービスコール要求、タイムアウト・エラーメッセージ、セッション・エラーメッセージ）は、クレジット決済端末からマーチャントプロセスに送られるメッセージを、23508の欄のメッセージ（認証テストA、認証テストB（答、認証テスト



トCの客、リモーターがケビニター、データーアッパ  
ーに寄る。アッパデータセンター、データーアッパ  
ーは、施設停止命令、借用照会客者、技師完了通知、キヤ  
ンセル完了通知、顧客サービスコール完了、呼び出し状  
書、問い合わせコール、タイムアウト・エラ一メッセ  
ージ、セブジョ・エラーメッセージ、タイムアウト・メ  
ッセージは、データベースからクルシット決  
算結果に送られるメッセージを示している。これ以外の  
メッセージを送っても、お互いに、有効なメッセージとし  
て解釈されない。

[10752] また、チリメンプロセルとチリメンサビは、同様のプロセスに属するサブ・プロセス。28693は、同様のプロセスに属69の23903及び23910の欄に示すサブ・プロセスをインポート・サービスとして提供する。23903の欄のメッセージ（使用照会応答）は、処理完了通知、キャンセルした通知、顧客サブ・プログラム応答、呼び出し応答、問い合わせコール、タイムアウト、エラー・メッセージ、センシティブ・エラール・メッセージ）は、サブ・プロセス・タイクログスからマニファクトリアルセクタに送られる。メッセージを、23910の欄のメッセージ（決断完了通知、キャンセル完了通知、顧客サブ・プロセスコール応答、呼び出し応答、問い合わせコール、タイムアウト、エラー・メッセージ、センシティブ・エラール・メッセージ、タイクログ・メッセージ）は、マニファクトリアルセクタからサブ・プロセス・タイクログセクタに送る。このようにして、これらのメッセージを送ると、お互いに、別のメッセージとして解釈されない。

【075】さらに、「アーチヤントフロセス336031」、「アーチヤントフロセス336002」、「図6.9の233912の欄に示すメッセージをインターフェイスとして通信する、233912の欄のメッセージ（通信要求、キャンセル要求、顧客サービスコール要求、自身のフロセス消去要求）」、「アーチヤントフロセスにからサービス、アーチヤントフロセスに送られるメッセージを示して、また、図6.9の233912の欄（「アーチヤントフロセス生成、アーチヤントフロセス消去）」は、「サービス、アーチヤントフロセスのアーチヤントフロセスへの作用を示しており、サービス、アーチヤントフロセスが、アーチヤントフロセスの生成と消去を行なう、メッセージの内容については、後で詳しく説明する。」

【705】「アーチャントフロセス」と他の「アーチャントフロセス」との間の通信のインタラクションは、直接「アーチャントフロセス」ではなく、他の「アーチャントフロセス」と、間接に、通信することはできない。同様に、「アーチャントフロセス」と「ユーザフロセス」、「アーチャントフロセス」と「検索処理機能フロセス」、「アーチャントフロセス」と異なる「プロセスグループ」の「サービス」、「チャイルドフロセス」との間の通信の「インタラクション」は、直接、「アーチャントフロセス」ではなく、「ユーザフロセス」、「検索処理機能フロセス」、及び異なる「プロセスグループ」の「サービス」、「チャイルドフロセス」

と、直接、通信することはできない。

【0755】次に、決済処理機関プロセス33804について説明する。

【0756】 決済処理機関プロセスは、決済システム101との通信制御と、決済処理機関の認証、決済システム103への送信データの暗号化、決済システム103からの受信データの復号化、決済システム103からの受信データの有効性のチェックを行なうプロセスである。

【075】決裁処理機関プロセス33804は、サービスタ提供システム103が決裁システム102と決裁されるプロセスである。サービスタ提供システム102と決裁システム103との間の1つ通信回線を用いた通信に対して、1つの決裁処理機関プロセス33804が生成される。サービスタ提供システム102と決裁システム103とを結ぶデジタル通信回線111は、多量度によって、複数の通信回線として動作する。したがって、サービスタ提供システム102と決裁システム103との間で、同時に、複数の通信回線を用いて動作する。この時、サービスタ提供システム33804は、通信回線に等しい数の決裁処理機関プロセス33804を生成する。この時、サービスタ提供システム33804は、サービスタサーバ400を構成するコンピュータのメモリ、または、ハードディスク上に、生成したそれぞれの決裁処理機関プロセスに対し、図75の(c)に示す決裁処理機関プロセス管理情報4403を生成して、決裁処理機関プロセスを管理する。

理機関ワロセ入管理情報102と、決済処理機関情報サーム401によって管理されている決済システム103が設置される決済処理機関の属性情報と決済処理の履歴情報とにアクセスするパーミッションが与えられ、逆に、決済処理機関ワロセ入1804は、その他の情報にアクセスすることはできない。

〔0759〕また、決裁処理機関プロセス33804は、決裁システム103に対してのみ有効なプロセスであり、その他の決裁システムと、直接、通信することはできない。

お支払い、有効なメッセージとして検閲されない、

【0761】また、決済処理機関プロセス23804は、同

ーのフロセスグループに属するサージェ、チャレクタ  
 ー(サージェ3880と、図6-9の33916及び33166の欄に示すマ  
 ッセージとエンタープライスとで通信する、33915の  
 欄のメッセージ、(決着要求、キヤンセル要求、タイムア  
 ウト、エアーメッセージ、セツジョ、エアーメッセージ)  
 は、サージェ、チャレクタグループから決着処理機  
 関フロセスに送られるメッセージを、33916の欄のメッ  
 セージ(決着完了通知、キヤンセル完了通知、セツジョ  
 ン、エアーメッセージ、タイムアウト、メッセージ)  
 は、決着処理機関フロセスからサージェ、チャレクタ  
 ーフロセスに送られるメッセージを示している。これ以外の  
 メッセージを送っても、お互いには有効なメッセージと  
 して解釈されない。

「0762」さらに、炭素処理装置でプロセス33804から、  
 サービス・マネージャプロセス33800と、図6.9の33918  
 の間に示すメッセージをインタフェースとして送付す  
 る。33918の欄のメッセージ（自身のプロセス消去要  
 求）は、炭素処理装置プロセスからサービス・マネー  
 ジャープロセスに送られるメッセージを示している。また、  
 図6.9の33917の欄（炭素処理装置プロセス生成、炭素  
 処理装置プロセス消去）は、サービス・マネージャプロ  
 セスの炭素処理装置プロセスへの作用を示しており、サ  
 ービス・マネージャプロセスが、炭素処理装置プロセス  
 の生成と消去を行なう。メッセージの内容については、  
 は、後で詳しく説明する。

「1076」は、読後処理管理プログラムと元の読後処理管理プログラムとの間の通信のインターフェースは、読後処理管理プログラムと、他の読後処理管理プログラムと、直接通信することはできない。同様に、読後処理管理プログラムとユーザプログラム、読後処理管理プログラムとデータベースプログラム、読後処理管理プログラムと異なるデータベースプログラムのサービス・チャイナプログラムとの間の通信のインターフェースは、ユーザプログラム、データベースプログラム、及び異なるデータベースプログラムのサービス・チャイナプログラムと、直接通信することはできない。

【0764】次に、サービス・ディレクタプロセス3801について説明する。

「10765」サービエ・デ・レヴァタラゴスは、同一の「アロセスグループ」に属するユザラゴス、マ・ヂ・チン・アロセス、及び汝波須理徳園「アロセス」それぞれ通信「アロセス」・リモント・クレジツツ・汝波サード・ビスを抽出する「アロセス」である。「バーチカル・リモント・クレジツツ・汝波サード」という表現は、サービエ・デ・レヴァタラゴスだが、同一の「アロセスグループ」の他のメンバー「アロセス」と連携して、「バーチカル・リモント・クレジツツ・汝波サード」の取組を主目的に行なうことを意図している。

【0766】サービス・ディレクタフロセス23801は、サービス提供システム102が、バーソナル・リモート・

[illegible]

【076】「バーンツル・リモート・クレジット決済カード」の「決断」「キャンセル」「顧客サポートセンター」の「問い合わせコーナー」の各項目は、それぞれ決まられた処理のシーケンスがある。サービス・デベロップメント・グループは、この決められた処理のシーケンスにしたがって、同のプログラム・オブジェクトをメンバークラスから送るのメッセージを受理し、また、各メンバークラスに対して、処理を促すメッセージを送る。サービス・デベロップメント・グループは、それぞれ、サービス・デベロップメント・グループから送られるメッセージに対して処理を行う。このように、サービス・デベロップメント・グループと、同のプログラム・オブジェクトのメンバークラスとが連携して処理を行うことによって、バーンツル・リモート・クレジット決済カードの処理が行なわれる。

〔0768〕“決壊”と“キヤンセル”との処理の場合には、サービス・チャリタツタロセんと、ユーザフロセと、サーチャントフロセと、及び決壊処理抽選フロセとが1つのフロセスグループとなつて、それぞれの処理を行ない、“決壊サービスコール”の処理と“問い合わせコール”の処理との場合には、サービス・チャリタツタロセんと、ユーザフロセと、及びサーチャントフロセとが1つのフロセスグループとなつて、それぞれの処理を行なふ。

このことはできない。

1170770) また、サービス・チャリタブル組織に属するユーザサービス33802と、図70の33904及び33905の欄に示すメッセージをインタフエイスとして提供する。33904の欄のメッセージ(支払要求、キャンセル要求、着信応答、問い合わせコール要求、タイムアウト、エラーメッセージ、セッション、エラーメッセージ、タイムアウト・メッセージ)は、ユーザサービスをめぐるサービス・ディレクトリカテゴリーに送られるメッセージを、33905の欄のメッセージ(領収書、キャンセル処理領収書、顧客サービスコー

ル、問い合わせコール来着、呼び出し来着、タイムアウト・エラーメッセージ、セッション・エラーメッセージは、サービス・ディレクタプロセスからユーザプロセスに送られるメッセージを示している。これ以外のメッセージを選んでも、お互いに、有効なメッセージとして解読されない。

【0771】同様に、サーバ・ビス・ディレクタプロセス2380は、同一のプロセスグループに属するマーチャントプロセス23803と、図70の23910及び23909の欄に示すメッセージをインタフエイスして通信する。23910の欄のメッセージは、決壊完了通知、キャンセル完了通知、顧客サービスコール依頼書、呼び出し依頼、問い合わせコール、タイムアウト、エラーメッセージ、セッション・エラーメッセージ、タイムアウト・メッセージ）、タイムアウト、エラーメッセージ、呼び出し依頼、問い合わせコール、タイムアウト、エラーメッセージ、セッション・エラーメッセージ、タイムアウト・メッセージ）は、マーチャントプロセスからサーバ・ビス・ディレクタプロセスに送られるメッセージを、23909の欄のメッセージ（情報照会依頼、決壊完了通知、キャンセル完了通知、顧客サービスコール依頼書、呼び出し依頼、問い合わせコール、タイムアウト、エラーメッセージ、セッション・エラーメッセージ）は、サーバ・ビス・ディレクタプロセスからマーチャントプロセスに送られるメッセージを示している。これ以外のメッセージを送っても、お互いに、有効なメッセージとして解釈されない。

【0772】同様に、サービズ・ディレクタプロセス2380は、同一のプロセスグループに属する決処理機四プロセス2380と、図70の23916及び23915の欄に示すメッセージをインポートフェイスとして題する。23916の欄のメッセージ（決処理完了通知、キャンセル完了通知、セッション・エラーメッセージ、タイムアウトメッセージ）は、決処理機四プロセスからサービズ・ディレクタプロセスに送られるメッセージを、23915の欄のメッセージ（決処理要求、キャンセル要求、タイムアウト・エラーメッセージ、セッション・エラーメッセージ）は、サービズ・ディレクタプロセスから決処理機四プロセスに送られるメッセージを示している。これ以外のメッセージを送っても、お互いに、有効なメッセージとして解釈されない。

【0773】さらに、サービス・ディレクタプロセス2380は、サービス・マネージャプロセス2380と、図70の2390の欄に示すメッセージをインターフェースとして送信する。2390の欄のメッセージ（メンバプロセス要求、プロセス消去要求）は、サービス・ディレクタプロセスからサービス・マネージャプロセスに送られるメッセージを示している。また、図70の2395の欄（サービス・ディレクタプロセス生成、サービス・ディレクタプロセス消去、支払要求、信用照会要求、キャンセル要求、顧客サービスコール要求、問い合わせ要求）は、サービス・マネージャプロセスのサービス・ディレクタプロセスへの作用とメッセージを示しており、サービス・マネージャプロセスが、サービス・ディレクタプロセス2390の欄に示すメッセージを送信する。

ロセスの生成と消去とを行なう。メッセージの内容について、様で詳しく説明する。

【0774】サービズ・ディレクタプロセスと異なるプロセスグループのエージェントプロセス、サービズ・ディレクタプロセスと異なるプロセスグループのマニファスタプロセス、サービズ・ディレクタプロセスと異なるプロセスグループの決裁処理機関プロセスとの間の通信のインターフェイスは、サービズ・ディレクタプロセスとは、異なるプロセスグループのエージェントプロセス、異なるプロセスグループのマニファスタプロセス、及び異なるプロセスグループの決裁処理機関プロセスと、直接、通信することではない。

【0775】次に、サービス・マネージャプロセス2380  
0について説明する。

【0776】サービス・マネージャプロセスは、ユーザプロセス33802、マーチャントプロセス33803、決済処理機関プロセス33804、及びサービス・ディレクタプロセス33801の生成と消去、並びに、プロセスグループの生成と消去を行なうプロセスである。

【0777】サーバ・ス・マネージャプロセス3800は、サーバ・ス・サ・バ400を構成するコンピュータのメモリ、または、ハードディスク上に、図75に示す、ユーザ・プロセス管理情報4400、マ・チャントプロセス管理情報4401、決処理情報4402、サーバ・ス・管理情報4403、プロセスグループ4404、及びメッセー・ジスト4405の6種類の管理データを生じ、各プロセスを管理する。プロセスグループ管理情報4404は、プロセスグループの管理データであり、メッセー・ジスト4405は、サーバ・ス・マネージャ・プロセスによって処理が保留されているメッセー・ジストである。メッセー・ジスト4405の役割については、後で詳しく説明する。

【0778】サー・ビス・マネージャプロセス23800は、サー・ビス提供システムがパーソナル・リモート・クレジット決済サービスを提供する場合に、常に、起動しているプロセスである。サー・ビス・マネージャプロセスの生成と消去は、管理システム407によって制御される。

【0779】また、サービス・マネージャブロッセス33800には、サービス・ディレクタ情報サーバ(40)によって管理されている情報にアクセスするパーミッションが与えられる。逆に、サービス・マネージャブロッセス23800は、その他の情報にアクセスすることはできない。

【0780】また、サービス・マネージャプロセス33900は、ユーザプロセス33801と、図70の33906の欄に示すメッセージをインターフェイスとして通信する。33900の欄のメッセージ（支払要求、キャンセル要求、問い合わせ要求、自身のプロセス消去要求）は、ユーザプロセスからサービス・マネージャプロセスに送られるメッセージを示している。また、図70の33905の欄（ユーザプロセス生成、ユーザプロセス消去）は、サービス・

マネージャプロセスのユーザプロセスへの作用を示しており、サービス・マネージャプロセスが、ユーザプロセスの生成と消去とを行なう。

【0781】同様に、サービス・マネージャプロセス33800は、マーチャントプロセス23803と、図70の33912の欄に示すメッセージをインターフェイスとして連携する。33912の欄のメッセージ（借用照会要求、キャンセル要求、顧客サービスコスト要求、自身のサービス・マネージャプロセスに送られるメッセージ）を示している。また、図70の33911の欄（マーチャントプロセス生成、マーチャントプロセス消去）は、サービス・マネージャプロセスのマーチャントプロセスへの作用を示しており、サービス・マネージャプロセスは、マーチャントプロセスの生成と消去を行なう。

【0782】同様に、サービス・マネージャプロセス33800は、決処理機関プロセス33804と、図70の33918の欄に示すメッセージをインターフェースとして選定する。33918の欄のメッセージ（自身のプロセス消去要求）は、決処理機関プロセスからサービス・マネージャプロセスに送られるメッセージを示している。また、図70の33917の欄（決処理機関プロセス生成、決処理機関プロセス消去）は、サービス・マネージャプロセスの決処理機関プロセスへの作用を示しており、サービス・マネージャプロセスが、決処理機関プロセスの生成と閉去を行なう。

【0783】同様に、サー・ビス・マネージャプロセス233800は、サー・ビス・ディレクタプロセス23800と、図70の23930の欄に示すメッセージをインターフェースとして処理する。23920の欄のメッセージ（メンバ・プロセス要求、プロセス消去要求）は、サー・ビス・ディレクタプロセスからサー・ビス・マネージャプロセスに送られるメッセージを示している。また、図70の23910の欄（サー・ビス・ディレクタプロセス生成、サー・ビス・ディレクタプロセス消去、支払要求、信用照会要求、キャンセル要求、顧客サー・ビスコール要求、問い合わせ要求）は、サー・ビス・マネージャプロセスのサー・ビス・ディレクタプロセスへの作用とメッセージを示しており、サー・ビス・マネージャプロセスが、サー・ビス・ディレクタプロセスの生成と消去を行なう。

【0784】また、サービス・マネージャプロセス33800は、他のサービスエリアのサービス提供システムのサービス・マネージャプロセスと、図70の33911及び33932の欄に示すメッセージをインターフェイスとして通信する。33921の欄のメッセージ（ユーザプロセス生成、ユーザプロセス消去、ホームユーザプロセス生成、ホームユーザプロセス消去、モバイルユーザプロセス生成、モバイルユーザプロセス消去、キャンセル要求、問い合わせコール要求）は、他のサービスエリアのサービス提供システムのサービス・マネージャプロセスからサービス

ス・マネージャプロセス38000に送られるメッセージ  
を、34932の別のメッセージ（ユーザプロセス生成、ユ  
ーザプロセス消去、ホムユーザプロセス生成、ホ  
ムユーザプロセス消去、モバイルユーザプロセス生  
成、モバイルユーザプロセス消去、キャンセル要求、開  
きコール要求）は、サービス・マネージャプロセス338  
00から他のサービスエリアのサービス提供システ  
ム（サービス・マネージャプロセス）に送られるメ  
ッセージを、異なるサービス提供システムのサー  
ビス・マネージャプロセスと同一の通信は、サー  
ビスエリアを跨って、パーソナル・リモート・ク  
レジット決済サービスを提供する場合に行なわれ  
る。これは、後で詳しく説明する。

【0785】次に、サービス提供システム102のユーザが情報サーバ402が管理する情報について説明する。ユーザが情報サーバ402は、ユーザの属性情報とユーザのパーソナル・クレジット端末100のRAM502のデータとを管理する。例えば、1つのユーザが情報サーバ402で、すべてのユーザの属性情報とパーソナル・クレジット端末100のRAM502のデータとを管理するわけではなく、サービス提供システム102はユーザの属性情報とユーザのパーソナル・クレジット端末100のRAM502のデータとを分散して管理する。したがって、ユーザが情報サーバ402は、サービス提供システム102が担当するサービスエリアに在住するユーザの属性情報とそのユーザのパーソナル・クレジット端末のRAMのデータとを管理する（以下では、ユーザが在住するサービスエリアをユーザの「ホームサービスエリア」と呼ぶ。）

【0786】図711は、一人のユーザに対して、ユーザ情報サーバ402に格納される情報を変化した模式図である。ユーザ情報サーバ402では、一人のユーザに対して、ユーザデータ管理情報2400、個人情報2401、写真データ2402、ターミナル・プロファイル2403、ユーザデータ2404、定情報2405、アクセス制御情報2405、端末データ2406、8、電話情報2407、クレジットカード・リスト2408、及び利用履歴リスト2409の10種類の情報が格納されている。これらの情報の詳しい内容は、第1の実施形態において、図29を用いて説明したものと同一である。

【01787】次に、サービス提供システム102のマーチャント情報サーバ403が管理する情報について説明する。マーチャント情報サーバ403は、マーチャントの属性情報とマーチャントのクレジット決済端末300のR/RAM21502とハードディスク21503のデータとを管理する。但し、1つのマーチャント情報サーバ403で、すべてのマーチャントの属性情報とクレジット決済端末のデータとを管理するわけではなく、サービスエリア毎に分散して管理する。したがって、マーチャント情報サーバ403は、サービス提供システム102が担当するサービスエリアに所在するマーチャントの属性情報とそのマーチャントのパーソナル・クレジット端末のRAMとハードディスクのデータとを管理する。

【0788】図72は、一つのマーチャントに対して、

(77)

ユーザチャント情報サーバ403に格納される情報を表した模式図である。ユーザチャント情報サーバ403では、一つのユーザチャントに対して、ユーザチャントデータ管理情報24100、ユーザチャント情報24101、タリミナル・プロパティ24102、ユーザチャント設定情報24103、宛先データ24104、電話情報24105、クレジットカード・リスト24106、及び既読履歴リスト24107の8種類の情報が格納されている。これらの情報の群し内容は、第1の実施形態において、図3.0を用いて説明したものと同一である。なお、ユーザチャント情報24101は、ユーザチャントの住所、口番番号、契約内容等のユーザチャントに関する情報であり、この情報の一画が、クレジット決済宛先24107のユーザチャント情報3506に示されている。

[0789] 次に、ユービス提供システム103の決済処理機関情報サーバ404が管理する情報について説明する。決済処理機関情報サーバ404は、決済処理機関の属性情報とその決済処理機関による決済処理の履歴情報とを管理する。

[0790] 図73は、一つの決済処理機関に対して、決済処理機関情報サーバ404に格納される情報を表した模式図である。決済処理機関情報サーバ404では、一つの決済処理機関に対して、決済処理機関データ管理情報24200、決済処理機関情報24201、クレジットカード・リスト24202、及び既読履歴リスト24203の4種類の情報が格納される。これらの情報の群し内容は、第1の実施形態において、図3.1を用いて説明したものと同一である。

[0791] 次に、ユービス提供システム103のサービスディレクタ情報サーバ401に格納される情報について説明する。

[0792] 図74は、サービスディレクタ情報サーバ401に格納される情報を表した模式図である。

[0793] サービスディレクタ情報サーバ401には、ユーザリスト4300、ユーザチャントリスト4301、決済処理機関リスト4302、ユービス提供履歴リスト4303、及び決済処理機関データ4304の5種類の情報が格納される。

[0794] ユーザリスト4300は、ユービス提供者と契約をしている全ユーザの属性情報を示し、ユービス提供者と契約をしている全決済処理機関の属性情報を示し、ユービス提供履歴リスト4303は、ユービス提供システム103が提供したパーソナル・リモート・クレジット決済サービスの履歴情報のリストであり、決済処理機関データ4304は、ユーザ及びユーザチャントからのパーソナル・リモート・クレジット決済サービスの要求に対して、最適な決済処理機関を対応付けたデータ情報である。

[0795] ユーザリスト4300には、一人のユーザに対して、ユーザ名4305(4310)、ユーザID4306(4311)、ユ

ーザ電話番号4307(4312)、サービス・リスト・アドレス4308(4313)、及びユーザ情報アドレス4309(4314)の5種類の情報が格納される。

[0796] サービス・リスト・アドレス4308(4313)は、ユーザが利用できるサービスコードのリストが格納されているアドレスを示し、ユーザ情報アドレス4309(4314)は、そのユーザのユーザデータ管理情報が格納されているアドレスを示す。ユーザが利用できるサービスコードのリストと、ユーザデータ管理情報とは、それぞれ、そのユーザのホームサーバベースのユービス提供システムにおけるサービスディレクタ情報サーバ10、ユービス提供サーバ10において管理される。したがって、ユービス提供システム103が、ユーザのホームサーバベースのユービス提供システムである場合には、サービス・リスト・アドレスと、ユーザ情報アドレスとは、それぞれ、サービスディレクタ情報サーバ10上のアドレスと、ユーザ情報サーバ10上のアドレスを示し、また、ユーザのホームサーバベースのユービス提供システム103のサービスエリアとが異なる場合には、サービス・リスト・アドレスと、ユーザ情報アドレスとは、それぞれ、ユーザのホームサーバベースのサービスエリアにおけるサービスディレクタ情報サーバ10上のアドレスと、ユーザ情報サーバ10上のアドレスを示す。

[0797] ユーザチャントリスト4301には、一つのユーザチャントに対して、ユーザチャント名4315(4321)、ユーザチャントID4316(4322)、ユーザチャント電話番号4317(4323)、サービス・リスト・アドレス4318(4324)、顧客データ・アドレス4319(4325)、及びユーザチャント情報アドレス4320(4326)の6種類の情報が格納される。

[0798] サービス・リスト・アドレス4308(4312)は、ユーザチャントが取り扱うことができるサービスコードのリストが格納されているアドレスを示し、顧客データ・アドレス4317(4322)は、顧客番号とユーザIDとを対応を示すユーザ情報(顧客データ)が格納されているアドレスを、ユーザチャント情報アドレス4320(4326)は、そのユーザチャントのユーザチャントデータ管理情報が格納されているアドレスを示す。

[0799] ユーザチャントが取り扱うことができるサービスコードのリスト及び顧客データと、ユーザチャントデータ管理情報とは、それぞれ、そのユーザチャントのホームサーバベースのサービスディレクタ情報サーバ10において管理される。したがって、ユービス提供システム103がユーザチャントのホームサーバベースのサービスエリアと異なる場合には、サービス・リスト・アドレスと、ユーザ情報アドレスとは、それぞれ、そのユーザのホームサーバベースのサービスエリアにおけるサービスディレクタ情報サーバ10上のアドレスを示し、また、ユーザチャントのホームサーバベースのサービスエリアと異なる場合には、サービス・リスト・アドレスと異なる場合には、

(78)

サービス・リスト・アドレスと顧客データ・アドレスとは、ユーザチャントのホームサーバベースのサービス提供システムにおけるサービスディレクタ情報サーバ10のアドレスを示し、ユーザ情報アドレスは、ユーザチャントのホームサーバベースのサービス提供システムにおけるユーザ情報サーバ10上のアドレスを示す。

[0800] 決済処理機関リスト4302には、一つの決済処理機関に対して、決済処理機関名4327(4332)、決済処理機関ID4328(4333)、決済処理機関通信ID4329(4334)、サービス・リスト・アドレス4330(4335)、及び決済処理機関情報アドレス4331(4336)の5種類の情報が格納される。

[0801] 決済処理機関通信ID4329(4334)は、サービス提供システム102が、ディレクタ通信回線111を介して決済システム103と通信する際の決済システム103のIDを示し、サービス・リスト・アドレス4330(4335)は、決済処理機関が取り扱うことができるサービスコードのリストが格納されているサービスディレクタ情報サーバ101上のアドレスを示し、決済処理機関情報アドレス4331(4336)は、その決済処理機関の決済処理機関データ管理情報が格納されている決済処理機関情報サーバ404上のアドレスを示す。

[0802] サービス提供履歴リスト4303には、パーソナル・リモート・クレジット決済サービスの一つのサービス提供に対して、サービス提供番号4337(4341)、サービスコード4338(4342)、サービス提供時刻4339(4343)、及びサービス提供情報アドレス4340(4344)の4種類の情報が格納される。

[0803] サービス提供番号4337(4341)は、一つのサービス提供におけるサービス提供システム102での処理をユーザに示す番号、サービスコード4338(4342)は、ユーザが利用したクレジットカードサービスの種類を示すサービス番号、サービス提供時刻4339(4343)は、パーソナル・リモート・クレジット決済サービスのサービスを提供した時刻、サービス提供情報アドレス4340(4344)は、一つのサービス提供におけるサービス提供システム102での処理の履歴情報が格納されているサービスディレクタ情報サーバ401上のアドレスを示す。

[0804] 次に、サービス・マネージャプロセス3800が、ユーザプロセス、ユーザチャントプロセス、決済処理機関プロセス、サービス・ディレクタプロセスを管理する際に生成するプロセスの管理データについて説明する。

[0805] 図75の(a)から(f)は、サービス・マネージャプロセスが生成するプロセスの管理データの構成を示している。

[0806] 図75 (a) は、一つのユーザプロセスに関して生成されるユーザプロセス管理情報4000のデータ構成を示している。ユーザプロセス管理情報4000は、ユーザプロセスのアドレスIDを示すユーザアドレスID

4406と、ユーザプロセスに対応するユーザのユーザID4407と、ユーザのホームサーバベースのサービスの提供システム上のユーザプロセスのアドレスIDを示すホームアドレスID4408と、ユーザのホームサーバベースのサービス以外のサービスエリアのサービス提供システム上のユーザプロセスのアドレスIDを示すモバイルアドレスID4409と、ユーザプロセスと同一のプロセスグループに属するサービス・ディレクタプロセスのアドレスIDを示すサービス・ディレクタプロセスのアドレスID4410と、ユーザプロセスの実行状態を示すプロセスステータス4411と、ユーザプロセスに割当てられたメモリ領域を示すプロセスデータ領域ポインタ4412の7種類の情報が構成される。

[0807] パーソナル・クレジット端末が、ユーザのホームサーバベースのサービス提供システムと通信する場合には、ホームサーバベースのサービス提供システムのサービス・マネージャプロセスは、パーソナル・クレジット端末に格納されているユーザプロセスID4406のフィールドには、すべてのサービスエリアのサービス提供システムを通して、ユーザにユーザプロセスを指示IDを決定し、ホームプロセスID4408とモバイルアドレスID4409のフィールドには、“0”を決定する。

[0808] 一方、ユーザが、ホームサーバベースのサービスエリアでパーソナル・クレジット端末を使用し、パーソナル・クレジット端末が、ホームサーバベースのサービス・マネージャプロセスと通信する場合には、パーソナル・クレジット端末に格納されているユーザプロセスID4406のフィールドには、パーソナル・クレジット端末が通信をするサービス提供システム上に生成される。

[0809] この場合、ホームサーバベースのサービス提供システム上のユーザプロセスを、ホームサーバプロセスIDP : Home User Process)と呼び、パーソナル・クレジット端末が通信をするサービス提供システム上のユーザプロセスを、モバイルユーザプロセスIDP : Mobile User Process)と呼び、ホームサーバプロセスと、モバイルユーザプロセスとは、お互いに通信をして、連携処理を行なう。一つのユーザプロセスとして機能する。具体的には、ホームサーバプロセスが、ユーザ情報サーバが管理するユーザの属性情報とユーザのパーソナル・クレジット端末のRAMのデータとにアクセスし、モバイルユーザプロセスが、パーソナル・クレジット端末との通信の頻度、及び、データ処理を行なう。つまり、モバイルユーザプロセスは、ホームサーバプロセスを介して、ユーザ情報サーバにアクセスする。

[0810] ホームサーバベースのサービス提供システム上のユーザプロセス・マネージャプロセスは、ホームサーバプロセスのユーザプロセス管理情報におけるユーザプロセスID4406のフィールドには、すべてのサービスエリア

(79)

アのサービス提供システムを通して、ユニークにホームユーザプロセスを指示IDを設定し、ホームプロセスID4408のフィールドには、“0”を、モバイルプロセスID4409のフィールドには、モバイルユーザプロセスのIDを設定する。

[0811] また、パーソナル・クレジット端末が通信をするサービス提供システム内のサービス・マネージャプロセスは、モバイルユーザプロセスのユーザプロセス管理情報4401におけるユーザプロセスID4406のフィールドには、すべてのサービスエリアのサービス提供システムを通して、ユニークにモバイルユーザプロセスを指示IDを設定し、ホームプロセスID4408のフィールドには、ホームユーザプロセスのIDを、モバイルプロセスID4409のフィールドには、“0”を設定する。

[0812] また、ユーザID4407と、サービス・ディレクタプロセスID4410とは、それぞれ、すべてのサービスエリアのサービス提供システムを通してユニークな、ユーザと、サービス・ディレクタプロセスを示す。

[0813] 次に、図75(b)は、1つのマーチャントプロセスに関連して生成されるマーチャントプロセス管理情報4401のデータ構成を示している。マーチャントプロセス管理情報4401は、マーチャントプロセスのアドレスIDを示すマーチャントプロセスID4413と、マーチャントプロセスに対応するマーチャントのマーチャントID4414と、マーチャントプロセスと同一のプロセスグループに属するサービス・ディレクタプロセスのプロセスIDを示すサービス・ディレクタプロセスID4415と、マーチャントプロセスの実行状態を示すプロセスID4416と、マーチャントプロセスに割当てられたメモリ領域を示すプロセスデータ領域ポインタ4417との5種類の情報で構成される。マーチャントプロセスID4413と、マーチャントID4414とは、それぞれ、すべてのサービスエリアのサービス提供システムを通してユニークな、マーチャントプロセスとマーチャントとサービス・ディレクタプロセスを示す。

[0814] 次に、図75(c)は、1つの決済処理機プロセスに関連して生成される決済処理機プロセス管理情報4402のデータ構成を示している。決済処理機プロセス管理情報4402は、決済処理機プロセスのプロセスIDを示す決済処理機プロセスID4418と、決済処理機プロセスに対応する決済処理機の決済処理機ID4419と、決済処理機プロセスと同一のプロセスグループに属するサービス・ディレクタプロセスのプロセスIDを示すサービス・ディレクタプロセスID4420と、決済処理機プロセスの実行状態を示すプロセスID4421と、決済処理機プロセスに割当てられたメモリ領域を示すプロセスデータ領域ポインタ4422との5種類の情報で構成される。決済処理機プロセスID

4418と、決済処理機ID4419と、サービス・ディレクタプロセスID4420とは、それぞれ、すべてのサービスエリアのサービス提供システムを通してユニークな、決済処理機プロセスと決済処理機とサービス・ディレクタプロセスを示す。

[0815] 次に、図75(d)は、1つのサービス・ディレクタプロセスに関連して生成されるサービス・ディレクタプロセス管理情報4403のデータ構成を示している。サービス・ディレクタプロセス管理情報4403は、サービス・ディレクタプロセスのプロセスIDを示すサービス・ディレクタプロセスID4423と、サービス・ディレクタプロセスが属するプロセスグループのIDを示すプロセスグループID4424と、サービス・ディレクタプロセスの発行状態を示すプロセスID4425と、サービス・ディレクタプロセスと同一のプロセスグループに属するプロセスのプロセスIDのリストを示すメンバーリスト4426と、サービス・ディレクタプロセスに割当てられたメモリ領域を示すプロセスデータ領域ポインタ4427との5種類の情報で構成される。サービス・ディレクタプロセスID4423とプロセスグループID4424とは、それぞれ、すべてのサービスエリアのサービス提供システムを通してユニークな、サービス・ディレクタプロセスとプロセスグループを示す。

[0816] 次に、図75(e)は、1つのプロセスグループに関連して生成されるプロセスグループ管理情報4404のデータ構成を示している。プロセスグループ管理情報4404は、プロセスグループのIDを示すプロセスグループID4428と、プロセスグループのサービス・ディレクタプロセスのプロセスIDを示すサービス・ディレクタプロセスID4429と、プロセスグループに属するプロセスのプロセスIDのリストを示すメンバーリスト4430との3種類の情報で構成される。プロセスグループID4428とサービス・ディレクタプロセスID4429とは、それぞれ、すべてのサービスエリアのサービス提供システムを通してユニークな、プロセスグループとサービス・ディレクタプロセスを示す。

[0817] 図75(f)は、サービス・マネージャプロセスによる処理が保留されているメッセージを示すメッセージリスト4405のデータ構成を示している。

[0818] サービス・マネージャプロセスに送られるメッセージの内、ユーザプロセスから送られる支払要求とキャンセル要求、及び、マーチャントプロセスから送られる信用照会要求とキャンセル要求は、処理が一時的に保留される場合があり、この場合に、サービス・マネージャプロセスによって、メッセージリスト4405に登録される。

[0819] 例えば、“決済”の処理の場合、支払要求が、信用照会要求よりも先にサービス・マネージャプロセスに送られる場合には、対応する信用照会要求が、サービス・マネージャプロセスに送られるまで、支払要求

(80)

はメッセージリスト4405に登録される。対応する信用照会要求がサービス・マネージャプロセスに送られると、サービス・マネージャプロセスは、サービス・ディレクタプロセスを生成し、生成されたサービス・ディレクタプロセスによって、支払要求と信用照会要求とが処理される。逆に、信用照会要求が、支払要求よりも先にサービス・マネージャプロセスに送られた場合には、対応する支払要求がサービス・マネージャプロセスに送られるまで、信用照会要求はメッセージリスト4405に登録される。対応する支払要求がサービス・マネージャプロセスに送られると、サービス・マネージャプロセスは、サービス・ディレクタプロセスを生成し、生成されたサービス・ディレクタプロセスによって、支払要求と信用照会要求とが処理される。

[0820] また、“キャンセル”の処理の場合、ユーザプロセスからのキャンセル要求が、マーチャントプロセスからのキャンセル要求よりも先にサービス・マネージャプロセスに送られる場合には、対応するマーチャントプロセスからのキャンセル要求が、サービス・マネージャプロセスに送られるまで、ユーザプロセスからのキャンセル要求はメッセージリスト4405に登録される。対応するマーチャントプロセスからのキャンセル要求がサービス・マネージャプロセスに送られると、サービス・マネージャプロセスは、サービス・ディレクタプロセスを生成し、生成されたサービス・ディレクタプロセスによって、ユーザプロセスとマーチャントプロセスとのキャンセル要求が処理される。逆に、マーチャントプロセスからのキャンセル要求が、ユーザプロセスからのキャンセル要求よりも先にサービス・マネージャプロセに送られた場合には、対応するユーザプロセスからのキャンセル要求が、サービス・マネージャプロセスに送られるまで、マーチャントプロセスからのキャンセル要求はメッセージリスト4405に登録される。対応するユーザプロセスからのキャンセル要求がサービス・マネージャプロセに送られると、サービス・ディレクタプロセスを生成し、生成されたサービス・ディレクタプロセスによって、ユーザプロセスとマーチャントプロセスとのキャンセル要求が処理される。

[0821] サービス・マネージャプロセスは、メッセージリスト4405に登録されているメッセージとメッセージの内容とを照合することによって、支払要求、信用照会要求、ユーザプロセス及びマーチャントプロセスからのキャンセル要求のそれぞれに対応するメッセージを抽出する。

[0822] メッセージリスト4405には、1つのメッセージに対して、メッセージへのポインタであるメッセージポインタ4431(4430)と、対応するメッセージを抽出する際に照合する照会データへのポインタである照会データポインタ4432(4435)と、メッセージの送り手のプロセ

スを示すプロセスID4433(4436)との3つの情報が登録される。

[0823] 次に、パーソナル・クレジット端末、または、クレジット決済端末によるサービス提供システムとのセッション確立の処理において交換されるメッセージの呼称について説明する。セッション確立の処理は、パーソナル・クレジット端末とサービス提供システム、または、クレジット決済端末とサービス提供システムとの間で通信を開始する前に、互いの相互認証を行なう処理である。以下では、この処理を、セッション確立処理と呼ぶ。

[0824] 図76は、パーソナル・クレジット端末からサービス提供システムに接続する場合のセッション確立処理の手順を示し、図78の(a)、(b)、(c)は、パーソナル・クレジット端末とサービス提供システムとの間で交換するメッセージの内容を示している。

[0825] また、図77は、サービス提供システムからパーソナル・クレジット端末に接続する場合のセッション確立処理の手順を示し、図78の(d)、(e)、(f)は、パーソナル・クレジット端末とサービス提供システムとの間で交換するメッセージの内容を示している。

[0826] パーソナル・クレジット端末からサービス提供システムに接続する場合、まず、パーソナル・クレジット端末100がサービス提供システム101に電話をかけ、回線接続する(回線接続4505)。この際、パーソナル・クレジット端末100は、デジタル公衆網108に、デジタル無線電話の回線接続を要求するメッセージ、発呼要求4506を送信し、デジタル公衆網108は、サービス提供システムを呼び出すメッセージ、発呼要求4507をサービス提供システムに送信する。それに対して、サービス提供システムは、呼び出しを許可するメッセージ、発呼応答4508をデジタル公衆網に送信し、デジタル公衆網は、回線接続を許可するメッセージ、発呼応答4509をパーソナル・クレジット端末に送信して、パーソナル・クレジット端末とサービス提供システムとは、回線で接続される(回線接続4509)。

[0827] この時、パーソナル・クレジット端末とデジタル公衆網、及び、デジタル公衆網とサービス提供システムとの間で交わされる発呼要求4506、発呼要求4507、発呼応答4508、発呼応答4509といったメッセージは、デジタル無線電話から伝送路109及び基地局104、デジタル通信回線107、デジタル公衆網108、デジタル通信回線105を介した回線接続のプロトコルに依存するものである。

[0828] また、サービス提供システムでは、サービス・マネージャプロセッサが、デジタル公衆網108からの発呼要求4501を受信する。サービス・マネージャプロセスは、発呼要求4501に含まれる、呼び手のパーソナル・

クレジット端末の電話番号情報から、呼び手のパーソナル・クレジット端末に接続するユーザプロセスを生成し(プロセス生成4602)、生成されたユーザプロセスが、着呼応答4603を生成して、パーソナル・クレジット端末と回線を接続する。

【0829】パーソナル・クレジット端末とユーザプロセスとの回線が接続されると(回線接続4605)、ユーザプロセスは、パーソナル・クレジット端末を認証するためのテストメッセージ、認証テストA4606を生成し、パーソナルクレジット端末に送信する。

【0830】図78(a)に示すように、認証テストA4606は、メッセージが認証テストA4606であることを示すヘッダ情報、認証テストAヘッダ4700と、任意のビットパターンであるテストパターンA4701をユーザの公開鍵で暗号化したもの4702とから成る。

【0831】パーソナル・クレジット端末は、認証テストA4606を受信し、テストパターンAの暗号をユーザのプライベート鍵で復号化して、認証テストA4606に対する応答メッセージであり、かつ、ユーザプロセスを認証するためのテストメッセージである、認証テストA応答4607を生成し、ユーザプロセスに送信する。

【0832】図78(b)に示すように、認証テストA応答4607は、メッセージが認証テストA応答4607であることを示すヘッダ情報、認証テストA応答ヘッダ4703と、暗号を復号化したテストパターンA4704と、任意のビットパターンであるテストパターンB4705をユーザの提供者の公開鍵で暗号化したもの4706とから成る。つまり、認証テストA応答4607には、テストパターンAに対する認証テストAに相当する、ユーザプロセスを認証するための認証テストBが含まれている。

【0833】ユーザプロセスは、認証テストA応答4607を受信し、テストパターンA4701を受信したテストパターンA4704とを照合して、ユーザを認証する。この場合のユーザの認証は、ユーザの公開鍵で暗号化されたテストパターンAは、ユーザのプライベート鍵を持つパーソナルクレジット端末でしか復号化できないという前提に基づいている。

【0834】ユーザプロセスは、さらに、テストパターンBの暗号をユーザの提供者のプライベート鍵で復号化して、認証テストBに対する応答メッセージ、認証テストB応答4608を生成し、パーソナル・クレジット端末に送信する。

【0835】図78(c)に示すように、認証テストB応答4608は、メッセージが認証テストB応答4608であることを示すヘッダ情報、認証テストB応答ヘッダ4707と、暗号を復号化したテストパターンB4708と、セッション許可メッセージ4709をユーザの公開鍵で暗号化したもの4710とから成る。セッション許可メッセージ4709は、パーソナルクレジット端末とのセッションを許可するメッセージであり、その中には、通信条件に関する情

報が含まれている。

【0836】パーソナル・クレジット端末は、認証テストB応答4608を受信し、テストパターンB4708を受信したテストパターンB4708とを照合して、ユーザプロセスを認証する。この場合のユーザプロセスの認証は、ユーザの提供者の公開鍵で暗号化されたテストパターンBは、ユーザの提供者のプライベート鍵を持つユーザの提供システムでしか復号化できないという前提に基づいている。

【0837】パーソナル・クレジット端末は、さらに、セッション許可メッセージの暗号をユーザのプライベート鍵で復号化して、ユーザプロセスとの通信条件をセッション許可メッセージの通信条件に設定する。

【0838】以上の処理によって、パーソナル・クレジット端末とユーザプロセスとは、お互いを相互に認証し、共通の通信条件に基づいて通信をするようになる(セッション確立4609)。この状態を、以下では、セッション確立状態と呼ぶ。

【0839】また、ユーザの提供システムからパーソナル・クレジット端末に接続する場合には、まず、ユーザの提供システム103が、パーソナル・クレジット端末100に電話をかけて、回線を接続する(回線接続4605)。この際、ユーザの提供システム103では、ユーザ・マネージャ4702が、回線を接続するパーソナルクレジット端末に接続するユーザプロセスを生成し(プロセス生成4600)、生成されたユーザプロセスを、デジタル公衆回線108に、デジタル無線電話の回線接続を要求するメッセージ、発呼要求4601を送信し、デジタル公衆回線108は、パーソナル・クレジット端末を呼び出すメッセージ、着呼要求4602を、パーソナル・クレジット端末に送信する。それに対して、パーソナル・クレジット端末は、呼び出しを許可するメッセージ、着呼応答4603を、デジタル公衆回線に送信し、デジタル公衆回線は、回線接続を許可するメッセージ、発呼応答4604をユーザプロセスに送信して、ユーザプロセスとパーソナル・クレジット端末とは、回線で接続される(回線接続4605)。この時、ユーザプロセスとデジタル公衆回線、及び、デジタル公衆回線とパーソナル・クレジット端末との間で交わされる発呼要求4601、着呼要求4602、着呼応答4603、発呼応答4604といったメッセージは、デジタル通信回線109及びデジタル公衆回線108、デジタル通信回線107、基地局104、伝送線106を介した回線接続のプロトコルに依存するものである。

【0840】ユーザプロセスとパーソナル・クレジット端末との回線が接続されると(回線接続4605)、パーソナル・クレジット端末は、ユーザプロセスを認証するためのテストメッセージ、認証テストC4606を生成し、ユーザプロセスに送信する。

【0841】図78(d)に示すように、認証テストC4606は、メッセージが認証テストC4606であることを示

すヘッダ情報、認証テストCヘッダ4711と、任意のビットパターンであるテストパターンC4712をユーザの提供者の公開鍵で暗号化したもの4713とから成る。

【0842】ユーザプロセスは、認証テストC4606を受信し、テストパターンCの暗号をユーザの提供者のプライベート鍵で復号化して、認証テストC4606に対する応答メッセージであり、かつ、パーソナル・クレジット端末を認証するためのテストメッセージである、認証テストC応答4607を生成し、パーソナル・クレジット端末に送信する。

【0843】図78(e)に示すように、認証テストC応答4607は、メッセージが認証テストC応答4607であることを示すヘッダ情報、認証テストC応答ヘッダ4714と、暗号を復号化したテストパターンC4715と、任意のビットパターンであるテストパターンD4716をユーザの公開鍵で暗号化したもの4717とから成る。つまり、認証テストC応答4607には、テストパターンCに対する認証テストCに相当する、パーソナル・クレジット端末を認証するための認証テストDが含まれている。

【0844】パーソナル・クレジット端末は、認証テストC応答4607を受信し、テストパターンC4715を受信したテストパターンC4715とを照合して、ユーザプロセスを認証する。この場合のユーザプロセスの認証は、ユーザの提供者の公開鍵で暗号化されたテストパターンCは、ユーザの提供者のプライベート鍵を持つユーザの提供システムでしか復号化できないという前提に基づいている。

【0845】パーソナル・クレジット端末は、さらに、テストパターンDの暗号をユーザのプライベート鍵で復号化して、認証テストDに対する応答メッセージ、認証テストD応答4608を生成し、ユーザプロセスに送信する。

【0846】図78(f)に示すように、認証テストD応答4608は、メッセージが認証テストD応答4608であることを示すヘッダ情報、認証テストD応答ヘッダ4718と、暗号を復号化したテストパターンD4719と、セッション許可メッセージ4720をユーザの公開鍵で暗号化したもの4721とから成る。セッション許可メッセージ4720は、ユーザプロセスとのセッションを許可するメッセージであり、その中には、通信条件に関する情報が含まれている。

【0847】ユーザプロセスは、認証テストD応答4608を受信し、テストパターンD4719を受信したテストパターンD4719とを照合して、パーソナル・クレジット端末を認証する。この場合のパーソナル・クレジット端末の認証は、ユーザの公開鍵で暗号化されたテストパターンDは、ユーザのプライベート鍵を持つパーソナル・クレジット端末でしか復号化できないという前提に基づいている。

【0848】ユーザプロセスは、さらに、セッション許

可メッセージの暗号をユーザの提供者のプライベート鍵で復号化して、パーソナル・クレジット端末との通信条件を、セッション許可メッセージの通信条件に設定する。

【0849】以上の処理によって、ユーザプロセスとパーソナル・クレジット端末とは、お互いを相互に認証し、共通の通信条件に基づいて通信をするようになり、セッション確立状態となる(セッション確立4609)。

【0850】クレジット決済端末とユーザの提供システムとのセッション確立処理は、パーソナル・クレジット端末とユーザの提供システムとのセッション確立処理と、全く同じ手順で行なわれる。

【0851】図79は、クレジット決済端末から、ユーザの提供システムに接続する場合のセッション確立処理の手順を示し、図81の(a)、(b)、(c)は、クレジット決済端末とユーザの提供システムとの間で交換するメッセージの内容を示している。

【0852】また、図80は、ユーザの提供システムからクレジット決済端末に接続する場合のセッション確立処理の手順を示し、図81の(d)、(e)、(f)で交換するメッセージの内容を示している。

【0853】クレジット決済端末から、ユーザの提供システムに接続する場合、まず、クレジット決済端末300が、ユーザの提供システム103に電話をかけて、回線を接続する(回線接続4605)。この際、クレジット決済端末300は、デジタル公衆回線108に、デジタル無線電話の回線接続を要求するメッセージ、発呼要求4600を送信し、デジタル公衆回線108は、発呼要求4601を、パーソナル・クレジット端末に送信し、着呼要求4602を、パーソナル・クレジット端末に送信する。それに対して、ユーザの提供システムは、呼び出しを許可するメッセージ、着呼応答4603をデジタル公衆回線に送信し、デジタル公衆回線は、回線接続を許可するメッセージ、発呼応答4604をクレジット決済端末に送信して、クレジット決済端末とユーザの提供システムとは、回線で接続される(回線接続4605)。

【0854】この時、クレジット決済端末とデジタル公衆回線、及び、デジタル公衆回線とユーザの提供システムとの間で交わされる発呼要求4600、着呼要求4601、着呼応答4603、発呼応答4604といったメッセージは、デジタル電話108、デジタル電話通信回線110及びデジタル公衆回線109、デジタル通信回線109を介した回線接続のプロトコルに依存するものである。

【0855】また、ユーザの提供システムでは、ユーザ・マネージャ4702が、回線を接続するパーソナル・クレジット端末に接続するユーザプロセスを生成し(プロセス生成4602)、生成されたユーザプロセスを、着呼

(83)

応答4803を送信して、クレジット決済端末と回線を接続する。

【0 8 5 6】クレジット決済端末とマーチャントプロセスとの回線が接続されると(回線接続4805)、マーチャントプロセスは、クレジット決済端末を認証するためのテストメッセージ、認証テストA4806を生成し、クレジット決済端末に送信する。

【0 8 5 7】図8 1 (a) に示すように、認証テストA4806は、メッセージが認証テストA4806であることを示すヘッダ情報、認証テストAヘッダ5000と、任意のビットパターンであるテストパターンA5001をマーチャントの公開鍵で暗号化したもの5002とから成る。

【0 8 5 8】クレジット決済端末は、認証テストA4806を受信し、テストパターンAの暗号をマーチャントのプライベート鍵で復号化して、認証テストA4806に対する応答メッセージであり、かつ、マーチャントプロセスを認証するためのテストメッセージである、認証テストA応答4807を生成し、マーチャントプロセスに送信する。

【0 8 5 9】図8 1 (b) に示すように、認証テストA応答4807は、メッセージが認証テストA応答4807であることを示すヘッダ情報、認証テストA応答ヘッダ5003と、暗号を復号化したテストパターンA5004と、任意のビットパターンであるテストパターンB5005をサービス提供者の公開鍵で暗号化したもの5006とから成る。つまり、認証テストA応答4807には、テストパターンAに対する認証テストAに相当する、マーチャントプロセスを認証するための認証テストBが含まれている。

【0 8 6 0】マーチャントプロセスは、認証テストA応答4807を受信し、テストパターンA5001と受信したテストパターンA5004とを照合して、マーチャントを認証する。この場合のマーチャントの認証は、マーチャントの公開鍵で暗号化されたテストパターンAは、マーチャントのプライベート鍵を持つクレジット決済端末でしか復号化できないという前提に基づいている。

【0 8 6 1】マーチャントプロセスは、さらに、テストパターンBの暗号をサービス提供者のプライベート鍵で復号化して、認証テストBに対する応答メッセージ、認証テストB応答4808を生成し、クレジット決済端末に送信する。

【0 8 6 2】図8 1 (c) に示すように、認証テストB応答4808は、メッセージが認証テストB応答4808であることを示すヘッダ情報、認証テストB応答ヘッダ5007と、暗号を復号化したテストパターンB5008と、セッション許可メッセージ5009をマーチャントの公開鍵で暗号化したもの5010とから成る。セッション許可メッセージ5009は、クレジット決済端末とのセッションを許可するメッセージであり、その中には、通信条件に関する情報が含まれている。

【0 8 6 3】クレジット決済端末は、認証テストB応答4808を受信し、テストパターンB5005と受信したテスト

パターンB5008とを照合して、マーチャントプロセスを認証する。この場合のマーチャントプロセスの認証は、サービス提供者の公開鍵で暗号化されたテストパターンBは、サービス提供者のプライベート鍵を持つサービス提供システムでしか復号化できないという前提に基づいている。

【0 8 6 4】クレジット決済端末は、さらに、セッション許可メッセージの暗号をマーチャントのプライベート鍵で復号化して、マーチャントプロセスとの通信条件をセッション許可メッセージの通信条件に変更する。

【0 8 6 5】以上の処理によって、クレジット決済端末とマーチャントプロセスとは、お互いを相互に認証し、共通の通信条件に基づいて通信をするようになり、セッション確立状態となる(セッション確立4809)。

【0 8 6 6】また、サービス提供システムから、クレジット決済端末に接続する場合には、まず、サービス提供システム102が、クレジット決済端末300に電話をかけ、回線を接続する(回線接続4905)。この際、サービス提供システム102では、サービス・マネージャプロセスが、回線を接続するクレジット決済端末に対応するマーチャントプロセスを生成し(プロセス生成4900)、生成されたマーチャントプロセスが、デジタル公衆網108に、デジタル電話の回線接続を要求するメッセージ、発呼要求4901を送信し、デジタル公衆網108は、クレジット決済端末を呼び出すメッセージ、発呼要求4902を、クレジット決済端末に送信する。それに対して、クレジット決済端末は、呼び出しを許可するメッセージ、発呼応答4903を、デジタル公衆網に送信し、デジタル公衆網は、回線接続を許可するメッセージ、発呼応答904をマーチャントプロセスに送信して、マーチャントプロセスとクレジット決済端末とは、回線で接続される(回線接続4905)。この時、マーチャントプロセスとデジタル公衆網、及び、デジタル公衆網とクレジット決済端末との間で交わされる発呼要求4901、発呼要求4902、発呼応答4903、発呼応答904といったメッセージは、デジタル公衆網109及びデジタル公衆網108、デジタル電話回線110を介した回線接続のプロトコルに依存するものである。

【0 8 6 7】マーチャントプロセスとクレジット決済端末との回線が接続されると(回線接続4905)、クレジット決済端末は、マーチャントプロセスを認証するためのテストメッセージ、認証テストC4906を生成して、マーチャントプロセスに送信する。

【0 8 6 8】図8 1 (d) に示すように、認証テストC4906は、メッセージが認証テストC4906であることを示すヘッダ情報、認証テストCヘッダ5011と、任意のビットパターンであるテストパターンC5012をサービス提供者の公開鍵で暗号化したもの5013とから成る。

【0 8 6 9】マーチャントプロセスは、認証テストC4906を受信し、テストパターンCの暗号をサービス提供者

(84)

のプライベート鍵で復号化して、認証テストC4906に対する応答メッセージであり、かつ、クレジット決済端末を認証するためのテストメッセージである、認証テストC応答4907を生成し、クレジット決済端末に送信する。

【0 8 7 0】図8 1 (e) に示すように、認証テストC応答4907は、メッセージが認証テストC応答4907であることを示すヘッダ情報、認証テストCヘッダ5014と、暗号を復号化したテストパターンC5015と、任意のビットパターンであるテストパターンD5016をマーチャントの公開鍵で暗号化したもの5017とから成る。つまり、認証テストC応答4907には、テストパターンCに対する認証テストCに相当する、クレジット決済端末を認証するための認証テストDが含まれている。

【0 8 7 1】クレジット決済端末は、認証テストC応答4907を受信し、テストパターンC5015と受信したテストパターンC5015とを照合して、マーチャントプロセスを認証する。この場合のマーチャントプロセスの認証は、サービス提供者の公開鍵で暗号化されたテストパターンCは、サービス提供者のプライベート鍵を持つサービス提供システムでしか復号化できないという前提に基づいている。

【0 8 7 2】クレジット決済端末は、さらに、テストパターンDの暗号をマーチャントのプライベート鍵で復号化して、認証テストDに対する応答メッセージ、認証テストD応答4908を生成し、マーチャントプロセスに送信する。

【0 8 7 3】図8 1 (f) に示すように、認証テストD応答4908は、メッセージが認証テストD応答4908であることを示すヘッダ情報、認証テストDヘッダ5018と、暗号を復号化したテストパターンD5019と、セッション許可メッセージ5020をサービス提供者の公開鍵で暗号化したもの5021とから成る。セッション許可メッセージ5020は、マーチャントプロセスとのセッションを許可するメッセージであり、その中には、通信条件に関する情報が含まれている。

【0 8 7 4】マーチャントプロセスは、認証テストD応答4908を受信し、テストパターンD5019と受信したテストパターンD5019とを照合して、クレジット決済端末を認証する。この場合のクレジット決済端末の認証は、マーチャントの公開鍵で暗号化されたテストパターンDは、マーチャントのプライベート鍵を持つクレジット決済端末でしか復号化できないという前提に基づいている。

【0 8 7 5】マーチャントプロセスは、さらに、セッション許可メッセージの暗号をサービス提供者のプライベート鍵で復号化して、クレジット決済端末との通信条件をセッション許可メッセージの通信条件に変更する。【0 8 7 6】以上の処理によって、マーチャントプロセスとクレジット決済端末は、お互いを相互に認証し、共通の通信条件に基づいて通信をするようになり、セッション

ョン確立状態となる(セッション確立4909)。

【0 8 7 7】次に、パーソナル・クレジット決済端末100、及び、クレジット決済端末300が、リモートアクセスの処理において、サービス提供システム102との間で交換するメッセージの内容について説明する。リモートアクセスの処理は、リモートアドレスに存在するデータをアクセスしようとした場合に、サービス提供システム102から、データをダウンロードする処理である。以下では、この処理を、リモートアクセス処理と呼ぶ。

【0 8 7 8】図8 2 (a) は、パーソナル・クレジット端末100によるリモートアクセス処理の手順を示し、図8 3 (a)、(b) は、パーソナル・クレジット端末100とユーザプロセスとの間で交換するメッセージの内容を示している。アクセスするデータが、リモートアドレスに存在する場合、パーソナル・クレジット端末100は、リモートアクセスプロセスを生成し、リモートアクセス処理を開始する。まず、サービス提供システム102とのセッションを確立して、サービス提供システム102のユーザプロセスにデータを要求するメッセージ、リモートアクセス要求5100を生成し、ユーザプロセスに送信する。

【0 8 7 9】図8 3 (a) に示すように、リモートアクセス要求5100は、メッセージがリモートアクセス要求5100であることを示すヘッダ情報、リモートアクセス要求ヘッダ5200と、リモートアドレスを示すデータアドレス5201と、ユーザID5202と、このリモートアクセス要求5100を発行した日時を示す発行日時5203とから成るデータについて、ユーザのデジタル署名5204を行ない、サービス提供者に封筒化したものである。

【0 8 8 0】サービス提供システム102のユーザプロセスは、リモートアクセス要求5100を受信し、暗号を復号化し、デジタル署名をチェックして、要求されたデータをパーソナル・クレジット端末100に送るメッセージ、リモートアクセスデータ5101を生成し、パーソナル・クレジット端末100に送信する。

【0 8 8 1】図8 3 (b) に示すように、リモートアクセスデータ5101は、メッセージがリモートアクセスデータ5101であることを示すヘッダ情報、リモートアクセスデータヘッダ5208と、要求されたデータ5209と、サービス提供者ID5210と、このリモートアクセスデータ5101を発行した日時を示す発行日時5211とから成るデータについて、サービス提供者のデジタル署名を行ない、ユーザに封筒化したものである。

【0 8 8 2】パーソナル・クレジット端末100は、リモートアクセスデータ5101を受信し、暗号を復号化し、デジタル署名をチェックして、テンポラリ領域に格納して、データにアクセスする。

【0 8 8 3】同様、図8 5 (a) は、クレジット決済端末300によるリモートアクセス処理の手順を示し、図8 6 (a)、(b) は、クレジット決済端末300とマー



(85)

チャントプロセスと間で交換するメッセージの内容を示している。アクセスするデータが、リモートプロセスに存在する場合、クレジット決済端末100は、リモートプロセスプロセスを生成し、リモートプロセス処理を開始する。まず、サービス提供システム102とのセッションを確立して、サービス提供システム103のアーチャントプロセスにデータを送るメッセージ、リモートプロセス要求5400を生成し、アーチャントプロセスに送信する。

[0884] 図86(a)に示すように、リモートプロセス要求5400は、メッセージがリモートプロセス要求5400であることを示すヘッダ情報、リモートプロセス要求ヘッダ5500と、リモートプロセスを示すデータプロセス5501と、アーチャントID5502と、このリモートプロセス要求5400を発行した日時を示す発行日時5503とから成るデータについて、アーチャントのデジタル署名5504を行ない、サービス提供者に封蔵化したものである。

[0885] サービス提供システム103のアーチャントプロセスは、リモートプロセス要求5400を受信し、暗号を復号化し、デジタル署名をチェッキングして、要求されたデータをクレジット決済端末100に送るメッセージ、リモートプロセスデータ5401を生成し、クレジット決済端末100に送信する。

[0886] 図86(b)に示すように、リモートプロセスデータ5401は、メッセージがリモートプロセスデータ5401であることを示すヘッダ情報、リモートプロセス要求ヘッダ5508と、要求されたデータ5509と、サービス提供者ID5510と、このリモートプロセスデータ5401を発行した日時を示す発行日時5511とから成るデータについて、サービス提供者のデジタル署名を行ない、アーチャント宛に封蔵化したものである。

[0887] クレジット決済端末100は、リモートプロセスデータ5401を受信し、暗号を復号化し、デジタル署名をチェッキングして、ランボウリ領域に格納して、データにアクセスする。

[0888] 次に、パーソナル・クレジット端末100、及び、クレジット決済端末100が、データアプリアード処理において、サービス提供システム102との間で交換するメッセージの内容について説明する。データアプリアード処理の処理は、サービス提供システムが、パーソナル・クレジット端末100のRAM502、または、クレジット決済端末のRAM2502及びハードディスク2503の内容を更新する処理である。以下では、この処理を、データアプリアード処理と呼ぶ。

[0889] 図82(b)は、パーソナル・クレジット端末100におけるデータアプリアード処理の手順を示し、図83(c)〜(f)と図84(a)は、パーソナル・クレジット端末100とサービス提供システム102との間で交換するメッセージの内容を示している。

(86)

ツカワシタの値が、アップデータ時刻レジスタに一致すると、データアプリアードプロセスを生成し、データアプリアード処理を開始する。パーソナル・クレジット端末100は、まず、サービス提供システム102とのセッションを確立して、サービス提供システム103のユーザプロセスにデータアプリアード処理を要求するメッセージ、データアプリアード要求5102を生成し、ユーザプロセスに送信する。

[0891] 図83(c)に示すように、データアプリアード要求5102は、メッセージがデータアプリアード要求5102であることを示すヘッダ情報、データアプリアード要求ヘッダ5310と、ユーザID5311と、このデータアプリアード要求5102を発行した日時を示す発行日時5318とから成るデータについて、ユーザのデジタル署名を行ない、サービス提供者に封蔵化したものである。

[0892] サービス提供システム103のユーザプロセスは、データアプリアード要求5102を受信し、暗号を復号化し、デジタル署名をチェッキングして、要求に対する暗号が由来であることを示すメッセージ、データアプリアード要求5103を生成し、パーソナル・クレジット端末100に送信する。

[0893] 図83(d)に示すように、データアプリアード要求5103は、メッセージがデータアプリアード要求5103であることを示すヘッダ情報、データアプリアード要求ヘッダ5323と、サービス提供者ID5324と、このデータアプリアード要求5103を発行した日時を示す発行日時5325とから成るデータについて、サービス提供者のデジタル署名を行ない、ユーザ宛に封蔵化したものである。

[0894] パーソナル・クレジット端末100は、データアプリアード要求5103を受信し、暗号を復号化し、デジタル署名をチェッキングし、RAM502のデータを、サービス提供システム102にアップロードするメッセージ、アップロードデータ5104を生成し、サービス提供システムに送信する。

[0895] 図83(e)に示すように、アップロードデータ5104は、メッセージがアップロードデータ5104であることを示すヘッダ情報、アップロードデータヘッダ5330と、RAM502のデータを圧縮したデータ、端末データ5331と、ユーザID5332と、このアップロードデータ5104を発行した日時を示す発行日時5333とから成るデータについて、ユーザのデジタル署名を行ない、サービス提供者に封蔵化したものである。

[0896] サービス提供システム103のユーザプロセスは、アップロードデータ5104を受信し、暗号を復号化し、デジタル署名をチェッキングして、圧縮された端末データ5331を解凍し、ユーザ情報サージナル上の端末データ14006、及び、その他のユーザデータ管理情報24000によって管理されるデータと照合する。

[0897] そして、新しい端末データを生成し、パーソナル・クレジット端末100のデータをアップデータするメッセージ、アップデータ5105を生成して、パーソナル・クレジット端末100に送信する。

[0898] 図83(f)に示すように、アップデータ5105は、メッセージがアップデータ5105であることを示すヘッダ情報、アップデータヘッダ5336とあることを示すヘッダ情報、アップデータヘッダ5338と、新しい端末データを圧縮したデータ、端末データ5339と、サービス提供者ID5340と、このアップデータ5105を発行した日時を示す発行日時5341とから成るデータについて、サービス提供者のデジタル署名を行ない、ユーザ宛に封蔵化したものである。

[0899] パーソナル・クレジット端末100は、アップデータ5105を受信し、暗号を復号化し、デジタル署名をチェッキングし、圧縮された端末データ5339を解凍して、RAM502のデータを更新する。

[0900] サービス提供システム102のユーザプロセスは、新しい端末データの生成において、複数データ領域218120の容量に余裕が無い場合には、各クレジットのアクセス時刻を比較し、アクセス時刻が最近のクレジットのアクセス時刻を割り当て、また、各利用情報の利用時刻を比較し、利用時刻が最近の利用情報の利用時刻を割り当て、また、パーソナル・クレジット端末のプログラムをバリエーションする必要がある場合には、基本プログラム領域のデータを更新する。

[0901] また、サービス提供システム103のユーザプロセスは、アップロードデータと端末データとを照合した際に、データの不正な改ざんが見られる場合は、アップロードデータ5105の代わりに、パーソナル・クレジット端末100の暗号を停止させるメッセージ、暗号停止命令5105を生成し、パーソナル・クレジット端末100に送信する。

[0902] 図84(a)に示すように、暗号停止命令5105は、メッセージが暗号停止命令5105であることを示すヘッダ情報、暗号停止命令ヘッダ5300と、サービス提供者ID5301と、この暗号停止命令5105を発行した日時を示す発行日時5302とから成るデータについて、サービス提供者のデジタル署名を行ない、ユーザ宛に封蔵化したものである。

[0903] この場合、暗号停止命令5105を受信したパーソナル・クレジット端末100は、暗号を復号化し、デジタル署名をチェッキングし、タミナル・ステータス1902を“使用不能”に変更して、使用不能状態になる。

[0904] このデータアプリアード処理によって、パーソナル・クレジット端末のRAMには、比較的に、使用不能で高い信頼性が格納され、パーソナル・クレジット端末のプログラムは、最新のバージョンに保たれ、また、端末データの不正な改ざんが防止される。

[0905] 同様に、図85(b)は、クレジット決済端末300におけるデータアプリアード処理の手順を示し、図86(c)〜(f)と図84(a)は、クレジット決済端末300とサービス提供システム102との間で交換するメッセージの内容を示している。

[0906] クレジット決済端末300は、クロックカウンタの値がアップデータ時刻レジスタに一致すると、データアプリアードプロセスを生成し、データアプリアード処理を開始する。クレジット決済端末300は、まず、サービス提供システム102とのセッションを確立して、サービス提供システム103のアーチャントプロセスにデータアプリアード処理を要求するメッセージ、データアプリアード要求5402を生成し、アーチャントプロセスに送信する。

[0907] 図86(c)に示すように、データアプリアード要求5402は、メッセージがデータアプリアード要求5402であることを示すヘッダ情報、データアプリアード要求ヘッダ5516と、アーチャントID5517と、このデータアプリアード要求5402を発行した日時を示す発行日時5518とから成るデータについて、アーチャントのデジタル署名を行ない、サービス提供者に封蔵化したものである。

[0908] サービス提供システム103のアーチャントプロセスは、データアプリアード要求5402を受信し、暗号を復号化し、デジタル署名をチェッキングして、要求に対する暗号が由来であることを示すメッセージ、データアプリアード要求5403を生成し、クレジット決済端末300に送信する。

[0909] 図86(d)に示すように、データアプリアード要求5403は、メッセージがデータアプリアード要求5403であることを示すヘッダ情報、データアプリアード要求ヘッダ5523と、サービス提供者ID5524と、このデータアプリアード要求5403を発行した日時を示す発行日時5525とから成るデータについて、サービス提供者のデジタル署名を行ない、アーチャント宛に封蔵化したものである。

[0910] クレジット決済端末300は、データアプリアード要求5403を受信し、暗号を復号化し、デジタル署名をチェッキングし、RAM2502とハードディスク2503とのデータを、サービス提供システム102にアップロードするメッセージ、アップロードデータ5404を生成し、サービス提供システムに送信する。

[0911] 図86(e)に示すように、アップロードデータ5404は、メッセージがアップロードデータ5404であることを示すヘッダ情報、アップロードデータヘッダ5530と、RAM2502とハードディスク2503とのデータを圧縮したデータ、端末データ5531と、アーチャントID5532と、このアップロードデータ5404を発行した日時を示す発行日時5533とから成るデータについて、アーチャントのデジタル署名を行ない、サービス提供者に封蔵化したものである。

【0912】サービス提供システム102のマーチャントプロセスは、アップロードデータ404を受信し、暗号を復号化し、デジタル署名をチェックする。そして、圧縮された暗号データ853を復号し、マーチャント情報データベース140上の暗号データ4104、及び、その他のマーチャントデータ管理情報4100によって管理されるデータと照合する。

【0913】そして、新しい端末データを生成し、クレジット決済端末300のデータをアップデートするメッセージ、アップデートデータ5405を生成して、クレジット決済端末300に送附する。

【0914】図 86 (1) に示すように、アップデータデータ4005は、メッセージがアップデータデータ4005であることを示すヘッダ情報、アップデータデータ4005のヘッダ情報、新しい端末データを正確化したデータ、端末データ6539と、サービス提供手段ID5540と、このアップデータデータ4005を発行した日時を示す発行日時5541とからなるデータについて、サービス提供者のデジタル署名を付加し、マーチャント別に符号化したものである。

【0915】クレジット決済端末3001は、アップデータ  
データ5405を受領し、暗号を復号化し、デジタル署名を  
チェックし、圧縮された端末データ5599を解凍して、R  
AM2502及びハードディスク2503のデータを更新す  
る。

【0916】サービス提供システム102のマーチャントプロセスは、新しい端末データの生成において、クレジットカード決済端末のハードディスク2503の容量に余裕が無  
い場合には、各販売情報の利用時刻を比較し、利用時刻が最近の販売情報の販売情報アドレスにローカルアドレスを割り当てる。また、クレジットカード決済情報のプログラムをバージョンアップする必要がある場合には、基本プログラム領域のデータを更新する。

【0917】また、サービス提供システム102のマーケティングプロセスは、アップロードデータと端末データとを照合した際に、データの不正な改ざんが検見された場合には、アップデータデータ508の代わりに、クレジット決済端末300の機能を停止させるメッセージ、機能停止命令505を生成し、クレジット決済端末300に送信する。

【0918】図87(a)に示すように、機能停止命令5405'は、メッセージが機能停止命令5405'であることを示すヘッダ情報、機能停止命令ヘッダ5400と、サービス提供者ID 5401と、この機能停止命令5405'を発行した日時を示す発行日時4602から成るデータについて、サービス提供者のデジタル署名を行ない、マーチャント宛に封筒化されたものである。

【0919】この場合、機能停止命令5405'を受信したクレジット決済端末300は、暗号を復号化し、デジタル署名をチェックし、ターミナル・ステータス22902を“使用不能”に変更して、使用不能状態になる。

【0927】そして、新しい婚床データを生成し、パーソナル・クレジット婚床100のデータをアップデイトするメッセージ、アップデイトデータ5108を生成して、パーソナル・クレジット婚床100に送信する。

【0928】パーソナル・クレジット端末100は、アップデータデータ5108を受領し、暗号を復号化し、デジタリ署名をチェックし、圧縮された端末データ5339を解凍して、RAM1509のデータを更新する。

【0929】また、サービス提供システム102のユーザープロセスは、アップロードデータと端末データとを照合した際に、データの不正な改ざんが発見された場合には、アップロードデータ5108の代わりに、パーソナル・クレジット端末データ5108の代わりに、パーソナル・クレジット端末100の機能を停止させるメッセージ、機能停止命令5108<sup>1</sup>を生成し、パーソナル・クレジット端末100に送信する。

【0930】この場合、技能停止命令「08」を受信したパーソナル・クレジット端末100は、暗号を復号化し、デジタル署名をチェックし、ターミナル・ステータス「902」を「使用不能」に変更して、使用不能状態になる。

【0931】同様に、図85(c)は、クレジット決済端末300における強制のデータアップグレード処理の手順を示し、図86(e)、(f)と図87(a)、(b)は、クレジット決済端末300とサービス提供システム102との間で交換するメッセージの内容を示している。

【0932】サービス提供システム101は、マーケティングと契約内容に変更があった場合など、クレジットカード決済未300のRAM及びハードディスクのデータを、早急に更新する必要がある場合、まず、クレジットカード決済未300とのセクションを確立し、クレジットカード決済未300に強制的数据アップデータ処理を命令するメッセージ、データアップデータ命令540を生成し、クレジットカード決済未300に送信する。

【0933】図84 (b) に示すように、データアップ  
データ命令406は、メッセージがデータアップデータ  
命令408であることを示すヘッダ情報、データアップデータ  
命令ヘッダ5607と、サービス提供者ID 5609と、この  
データアップデータ命令408を発行した日時を示す発行  
日時5609とから成るデータについて、サービス提供者の  
デジタル署名を行ない、マージチャート列に追加化したも  
のである。

【0934】クレジットカード300は、データアップロード命令508を受信し、暗号を復号し、デジタル署名をチェックし、強制的データアップロードプロセスを生成し、強制的データアップロード処理を開始する。クレジットカード300は、まず、RAMとハードディスクのデータを、サービス提供システム102にアップロードするメッセージ、アップロードデータ540を生成し、サービス提供システム102に送信する。

【0935】サービス提供システム102のマーケティングプロセスは、アップロードデータ540を受信し、暗号を

【0920】このデータアップデイト処理によって、ク  
レジット決済済みのRAM、及び、ハードディスクに  
は、比較的、使用頻度が高い情報が格納され、クレジッ  
ト決済済みのプログラムは、最新のバージョンに保た  
れ、また、顧客データの不正な改ざんが防止される。

【0921】次に、パーソナル・クレジット端末100、及び、クレジット決済機300が、強制データアップデートの処理において、サービス提供システム102との間で交換メッセージの内容について説明する。強制データのアップデートの処理は、パーソナル・クレジット端末100のRAM1502、または、クレジット決済機300のRAM2502及びハードディスク32503の内容を、早急に更新する必要がある場合に、サービス提供システム102が、これらを強制に更新する処理である。以下では、この処理を、強制データアップデート処理と呼ぶ。

端末100における強制のデータアップデート処理の手順【0922】図82(c)は、パーソナル・クレジットカード100における強制のデータアップデート処理の手順を示し、図83(e)、(f)と図84(a)、(b)を示す。ここでは、パーソナル・クレジット端末100とサービス提供システム103との間で交換するメッセージの内容を示している。

【0923】サーバ型提供システム102は、ユーザとの契約内容に変更があった場合など、パーソナル・クレジット端末100のRAMのデータを早急に更新する必要がある場合、まず、パーソナル・クレジット端末100とのセッションを確立して、パーソナル・クレジット端末100に強制のデータアップデート処理を命令するメッセージ、データアップデート命令5100を生成し、パーソナル・クレジット端末100に送信する。

【0924】図 8.4 (b) に示すように、データアップ  
データ命令S1008は、メッセージがデータアップデータ  
命令S1005であることを示すヘッダ情報、データアップ  
データ命令ヘッダS307と、サービス提供者ID S308と、この  
データアップデータ命令S1008を発行した日時を示す発行  
日時S309とから成るデータについて、サービス提供者の  
デジタル署名を行ない、ユーザ宛に封装化しものである。

【0925】パーソナル・クレジット増大100は、データアップグレード命令5108を受信し、暗号を復号化し、デジタル署名をチェックし、強制制データアップグレードプロセスを生成して、強制制データアップグレード処理を開始する。パーソナル・クレジット増大100は、まず、R-AM1502のデータをサーバ上で提供システム102にアップロードするメッセージ、アップグレードシステム107を生成し、サーバ提供システム102に送信する。

【0926】サービス提供システム102のユーザプロセスは、アップロードデータ5107を受領し、暗号を復号化し、デジタル署名をチェックする。そして、圧縮された婦来データ5231を解凍し、ユーザ情報サーバ402上の婦来データ24008と照合する。



09を生成し、ユーザプロセスに送信する。

【0943】 サービス提供システム103のユーザプロセスは、デジタラデータ要求5109を受信し、暗号を復号化し、デジタル署名をチェックして、要求に対する暗号が出力されることを示すメッセージ、デジタラデータ要求5110を生成し、パーソナル・クレジット端末100に送信する。

【0944】 パーソナル・クレジット端末100は、デジタラデータ要求5110を受信し、暗号を復号化し、デジタル署名をチェックし、RAM1503のデータをサービス提供システム102にアップロードするメッセージ、アップロードデータ5111を生成し、サービス提供システムに送信する。

【0945】 サービス提供システム102のユーザプロセスは、アップロードデータ5111を受信し、暗号を復号化し、デジタル署名をチェックする。そして、圧縮された端末データ5131を解凍し、ユーザ情報サービス1402上の端末データ34006と照合する。

【0946】 そして、新しい端末データを生成し、パーソナル・クレジット端末100のデータをアップロードするメッセージ、アップロードデータ5112を生成し、パーソナル・クレジット端末100に送信する。

【0947】 パーソナル・クレジット端末100は、アップロードデータ5112を受信し、暗号を復号化し、デジタル署名をチェックし、圧縮された端末データ5133を解凍して、RAM1503のデータを更新する。さらに、タイムスタンプ512903を“書き込み不可”に変更して、パッチデータの管理が十分な状態になるまで、RAMへの新たなデータの入力を禁止する。

【0948】 また、サービス提供システム102のユーザプロセスは、アップロードデータと端末データとを照合した際に、データの不正な改ざんが検出された場合には、アップロードデータ5113の代わりに、パーソナル・クレジット端末100の機能を停止させるメッセージ、機能停止命令5114を生成し、パーソナル・クレジット端末100に送信する。

【0949】 この場合、機能停止命令5114を受信したパーソナル・クレジット端末100は、暗号を復号化し、デジタル署名をチェックし、タイムスタンプ512902を“使用不能”及び“書き込み不可”に変更して、使用不能状態になる。

【0950】 次に、“決済”の処理において、機器間で交換されるメッセージの内容について説明する。

【0951】 図88は、“決済”の処理における機器間のメッセージ交換の手順を示し、図91(a)～(f)、図90(a)～(c)、図91(a)～(b)は、“決済”の処理において、機器間で交換するメッセージの内容を示している。図88は、図43から、機器間で交換するメッセージの部分を抜き出した図であり、図88と図43は、同じ“決済”の処理を示している。

【0952】 まず、ユーザチャントが、レジスタのクレジット決済スイッチを押す5004と、クレジット決済端末300は、決済プロセスを生成して、“決済”の処理を開始する。クレジット決済端末300は、複数種類の支払オフナー要求5701(20609)を生成し、支払オフナー5700の受信待ち状態となる。

【0953】 次に、ユーザが、支払操作70607をする。と、パーソナル・クレジット端末100は、決済プロセスを生成して、“決済”の処理を開始する。パーソナル・クレジット端末100は、支払オフナー5700(20609)を生成し、赤外線通信で、クレジット決済端末300に送信する。

【0954】 図89(a)に示すように、支払オフナー5700は、メッセージが支払オフナー5700であることを示すヘッダ情報、支払オフナーヘッダ5800と、サービスコード5801と、サービス提供者ID5802と、ユーザチャントとの取引をユニークに示す番号として任意に生成した要求番号5803と、ユーザが入力した支払金額5804と、ユーザが入力した支払オフションを示す支払オフションコード5805と、この支払オフナー5808の有効期間5806と、この支払オフナー5808を発行した日時を示す発行日時5807とから成るデータについて、ユーザのデジタル署名を行なったものである。

【0955】 支払金額と請求金額とを照合し、支払オフション5805が利用可能なオフションであるか否かを照合して、複数種類の支払オフナー要求5701の中から、適当な支払オフナー要求5701を選択して、赤外線通信でパーソナル・クレジット端末100に送信し、さらに、信用照会要求5702(20610)を生成し、デジタル電話通信でサービス提供システム102のユーザチャントプロセスに送信する。

【0956】 図89(b)に示すように、支払オフナー要求5701は、メッセージが支払オフナー要求5701であることを示すヘッダ情報、支払オフナーヘッダ5808と、パーソナル・クレジット端末100が支払オフナー要求5701を受信した際にLCD503に表示される応答メッセージ5809と、ユーザとの取引をユニークに示す番号として任意に生成したトランザクション番号5810と、請求金額5811と、ユーザチャントのサービスエリアのサービス提供システムの電話番号を示すサービス提供電話番号5812と、この支払オフナー要求5701の有効期間5813と、ユーザチャント1D5814と、この支払オフナー要求5701を発行した日時を示す発行日時5815とから成るデータについて、サービス提供者のデジタル署名を行なったものである。サービス提供者の電話番号5813には、サービス提供者のデジタル署名がされており、また、応答メッセージ5808は、ユーザチャントのオフショントで設定するテキストメッセージであり、設定されない場合もある。

【0957】 図89(c)に示すように、信用照会要求

5702は、メッセージが信用照会要求5702であることを示すヘッダ情報、信用照会要求ヘッダ5816と、支払オフナー5700と、支払オフナー要求5701と、担当者名5817と、ユーザチャント1D5818と、この信用照会要求5702を発行した日時を示す発行日時5819とから成るデータについて、ユーザチャントのデジタル署名を行ない、サービス提供者側に封筒化したものである。担当者名5817は、ユーザチャントのオフショントで設定する情報であり、設定されない場合もある。

【0958】 一方、パーソナル・クレジット端末100は、支払オフナー要求5701を受信し、支払金額5804と請求金額5811とを照合して、支払要求5703(20613)を生成し、デジタル無線電話通信で、サービス提供システム102のユーザプロセスに送信する。

【0959】 図89(d)に示すように、支払要求5703は、メッセージが支払要求5703であることを示すヘッダ情報、支払要求ヘッダ5824と、支払オフナー5700と、支払オフナー要求5701と、ユーザID5825と、この支払要求5703を発行した日時を示す発行日時5826とから成るデータについて、ユーザのデジタル署名を行ない、サービス提供者側に封筒化したものである。

【0960】 クレジット決済端末300による信用照会要求5702のユーザチャントプロセスへの送信と、パーソナル・クレジット端末による支払要求5703のユーザプロセスへの送信は、どちらが先に行なわれてもよく、同時であってもよい。

【0961】 サービス提供システム102のユーザチャントプロセス及びユーザプロセスは、それぞれ、信用照会要求5702と支払要求5703を受信し、暗号を復号化し、デジタル署名をチェックして、それぞれ、信用照会要求5820と支払要求5827とをサービス・マネージャプロセスに送る。サービス・マネージャプロセスは、要求番号とトランザクション番号とユーザチャントIDとを照合して、信用照会要求と支払要求との対応をとり、サービス・チャレクタプロセスを生成して、信用照会要求5820と支払要求5827とを処理するプロセスルーチアを生成する。サービス・チャレクタプロセスは、信用照会要求5702と支払要求5703の内容を照合し、ユーザの信用照会を行なう。信用照会応答5840を生成し、ユーザチャントプロセスが、これをユーザチャント側に封筒化し、信用照会応答5704(20614)として、デジタル電話通信で、クレジット決済端末300に送信する。

【0962】 図89(e)に示すように、信用照会応答5704は、メッセージが信用照会応答5704であることを示すヘッダ情報、信用照会応答ヘッダ5831と、トランザクション番号5832と、信用照会の処理をユニークに示す番号として任意に生成した照会番号5833と、信用照会の結果を示す照会結果5834と、ユーザの氏名とユーザの年齢情報とユーザの顔の写真データとから成るユーザ個人データ5835と、ユーザチャントに対してユーザをユニークに

示す照会番号5836と、この信用照会応答5704の有効期間を示す有効期間5837と、サービス提供者ID5838と、この信用照会応答5704を発行した日時を示す発行日時5839とから成るデータについて、サービス提供者のデジタル署名を行ない、ユーザチャント側に封筒化したものである。信用照会の結果、ユーザの信用状況に問題がある場合は、ユーザ個人情報5834は設定されず、また、照会番号5836は、ユーザとユーザチャントとの間で、以前に、パーソナル・リセプト・クレジット決済サービスによる取引があった場合に設定される。

【0963】 クレジット決済端末300は、信用照会応答5704を受信し、暗号を復号化し、デジタル署名をチェックして、信用照会の結果をLCD3032に表示する。

【0964】 次に、ユーザチャントの担当者が、決済処理要求操作70616を行なうと、クレジット決済端末300は、決済要求5705(20618)を生成し、デジタル電話通信で、ユーザチャントプロセスに送信する。

【0965】 図89(f)に示すように、決済要求5705は、メッセージが決済要求5705であることを示すヘッダ情報、決済要求ヘッダ5844と、支払オフナー5700と、支払オフナー要求5701と、サービス提供システム102が発行した照会番号5845と、この決済要求5705の有効期間を示す有効期間5846と、担当者名5847と、ユーザチャントID5848と、この決済要求5705を発行した日時を示す発行日時5849とから成るデータについて、ユーザチャントのデジタル署名を行ない、サービス提供者側に封筒化したものである。担当者名5847は、ユーザチャントのオフションで設定する情報であり、設定されない場合もある。

【0966】 サービス提供システム102のユーザチャントプロセスは、決済要求5705を受信し、暗号を復号化し、デジタル署名をチェックして、決済要求のメッセージをサービス・チャレクタプロセスに送る。サービス・チャレクタプロセスは、決済要求5705と支払要求5700との内容を照合して、決済処理規則に対する決済要求5806を生成し、決済処理規則プロセスが、これを決済処理規則に封筒化し、決済要求5806(20619)として、決済システムに送信する。

【0967】 図90(a)に示すように、決済要求5706は、メッセージが決済要求5706であることを示すヘッダ情報、決済要求ヘッダ5900と、ユーザが指定したサービスコードに対応するクレジット番号5901と、パーソナル・クレジット端末100が発行した要求番号5902と、支払金額5903と、支払オフションコード5904と、ユーザチャントの口座番号を示すユーザチャント・アカウント番号5905と、クレジット決済端末300が発行したトランザクション番号5906と、この決済要求5706の有効期間を示す有効期間5907と、サービス提供者ID5908と、この決済要求5706が発行した日時を示す発行日時5909とから成るデータについて、サービス提供者のデジタル署名を行ない、決済処理規則に封筒化したものである。

(91)

【0968】決済システム103は、決済要求5706を受信し、暗号を復号化し、デジタル署名をチェックして、決済処理を行なう。そして、決済完了通知5707(20650)を生成し、サービス提供システム103に送信する。

【0969】図90(b)に示すように、決済完了通知5707は、メッセージが決済完了通知5707であることを示すヘッダ情報、決済完了通知5707と、決済システム103の決済処理をユニークに示す番号としたユーザ向け決済情報5915と、クレジットカード番号5916と、要求番号5917と、支払金額5918と、支払オプションコード5919と、マーチャント・アカウント番号5920と、トランザクション番号5921と、決済処理機関のデジタル署名をしたサービス提供者向け決済情報5922と、決済処理機関のデジタル署名をしたマーチャント向け決済情報5923と、決済処理機関のデジタル署名をしたユーザ向け決済情報5924と、決済処理機関ID5925と、この決済完了通知を発行した日時を示す発行日時5926とから成るデータについて、決済処理機関のデジタル署名を行ない、サービス提供者宛に封鎖化したものである。

【0970】サービス提供システム103の決済処理機関プロセスは、決済完了通知5707を受信し、暗号を復号化し、デジタル署名をチェックして、決済完了通知5927をサービス・ディレクタプロセスに送る。サービス・ディレクタプロセスは、決済完了通知5927から、マーチャントに対する決済完了通知5937を生成し、マーチャントプロセスが、これをマーチャント宛に封鎖化し、マーチャントに対して、決済完了通知5708(20651)として、デジタル電話通信で、クレジット決済端末300に送信する。

【0971】図90(c)に示すように、決済完了通知5708は、メッセージが決済完了通知5708であることを示すヘッダ情報、決済完了通知ヘッダ5931と、決済番号5932と、決済処理機関のデジタル署名をしたマーチャント向け決済情報5933と、マーチャントに対して、ユーザをユニークに示す番号として生成した番号、顧客番号5933と、暗号を復号化した決済要求5935と、サービス提供システム103における処理に関する情報を示すサービス提供者処理情報5934と、サービス提供者ID5935と、この決済完了通知5708を発行した日時を示す発行日時5936とから成るデータについて、サービス提供者のデジタル署名を行ない、マーチャント宛に封鎖化したものである。サービス提供者処理情報5934は、サービス提供者のオプションで設定する情報であり、設定されない場合もある。

【0972】クレジット決済端末300は、決済完了通知5708を受信し、暗号を復号化し、デジタル署名をチェックして、領収書5709(20682)を生成し、デジタル電話通信で、マーチャントプロセスに送信する。

【0973】図91(a)に示すように、領収書5709は、メッセージが領収書5709であることを示すヘッダ情報、領収書ヘッダ6000と、販売した商品の名前を示す商

品名6001と、マーチャントからユーザへの取引に関する付加情報を示す販売情報6002と、決済番号6003と、トランザクション番号6004と、支払オプファア5700と、担当者名6005と、マーチャントID6006と、この領収書5709を発行した日時を示す発行日時6007とから成るデータについて、マーチャントのデジタル署名を行ない、サービス提供者宛に封鎖化したものである。販売情報6002と担当者名6005とは、マーチャントのオプションで設定する情報であり、設定されない場合もある。

【0974】サービス提供システム103のマーチャントプロセスは、領収書5709を受信し、暗号を復号化し、デジタル署名をチェックして、領収書6008をサービス・ディレクタプロセスに送る。サービス・ディレクタプロセスは、領収書6008から、ユーザに対する領収書6016を生成し、ユーザプロセスが、これをユーザ宛に封鎖化し、領収書5710(20624)として、デジタル無線電話通信で、パーソナル・クレジット端末100に送信する。

【0975】図91(b)に示すように、領収書5710は、メッセージが領収書5710であることを示すヘッダ情報、領収書ヘッダ6012と、暗号を復号化した領収書6008と、決済処理機関のデジタル署名をしたユーザ向け決済情報5924と、サービス提供システム103における処理に関する情報を示すサービス提供者処理情報6013と、サービス提供者ID6014と、この領収書5710を発行した日時を示す発行日時6015とから成るデータについて、サービス提供者のデジタル署名を行ない、ユーザ宛に封鎖化したものである。サービス提供者処理情報6013は、サービス提供者のオプションで設定する情報であり、設定されない場合もある。

【0976】パーソナル・クレジット端末100は、領収書5710を受信し、暗号を復号化し、デジタル署名をチェックして、その内容をLCD203に表示する。

【0977】次に、“キャンセル”の処理において、機器間で交換されるメッセージの内容について説明する。【0978】図92は、“キャンセル”の処理における機器間のメッセージ交換の手順を示し、図93(a)～(f)は、“キャンセル”の処理において、機器間で交換するメッセージの内容を示している。図92は、図9から、機器間で交換するメッセージの部分を抜き出した図であり、図92と図9は、同じ“キャンセル”の処理を示している。

【0979】まず、マーチャントの担当者が、キャンセル操作301を行なうと、クレジット決済端末300は、キャンセルプロセスを生成し、“キャンセル”の処理を開始する。クレジット決済端末300は、キャンセルする取引の決済完了通知から、キャンセル要求6100(9003)を生成し、デジタル電話通信で、サービス提供システム103のマーチャントプロセスに送信する。【0980】一方、ユーザが、キャンセル操作301を行なうと、パーソナル・クレジット端末100は、キャンセ

(92)

ルプロセスを生成し、“キャンセル”の処理を開始する。パーソナル・クレジット端末100は、キャンセルする取引の領収書から、キャンセル要求6101(9006)を生成し、デジタル無線電話通信で、サービス提供システム103のユーザプロセスに送信する。

【0981】図93(a)に示すように、キャンセル要求6100は、メッセージがキャンセル要求6100であることを示すヘッダ情報、キャンセル要求ヘッダ6200と、暗号を復号化した決済完了通知5937と、このキャンセル要求6100の有効期間を示す有効期間6201と、担当者名6202と、マーチャントID6203と、このキャンセル要求6100を発行した日時を示す発行日時6204とから成るデータについて、マーチャントのデジタル署名を行ない、サービス提供者宛に封鎖化したものである。担当者名6216は、マーチャントのオプションで設定する情報であり、設定されない場合もある。

【0982】また、図93(b)に示すように、キャンセル要求6101は、メッセージがキャンセル要求6101であることを示すヘッダ情報、キャンセル要求ヘッダ6209と、暗号を復号化した領収書6016と、このキャンセル要求6101の有効期間を示す有効期間6210と、ユーザID6211と、このキャンセル要求6101を発行した日時を示す発行日時6212とから成るデータについて、ユーザのデジタル署名を行ない、サービス提供者宛に封鎖化したものである。

【0983】クレジット決済端末100によるキャンセル要求6100のマーチャントプロセスへの送信と、パーソナル・クレジット端末100によるキャンセル要求6101のユーザプロセスへの送信とは、どちらが先に行なわれてもよく、同時であってもよい。

【0984】サービス提供システム103のマーチャントプロセス及びユーザプロセスは、それぞれ、キャンセル要求6100とキャンセル要求6101とを受信し、暗号を復号化し、デジタル署名をチェックして、それぞれ、キャンセル要求6205とキャンセル要求6213とをサービス・マネージャプロセスに送る。サービス・マネージャプロセスは、要求番号とトランザクション番号とマーチャントIDとを照合して、キャンセル要求6205とキャンセル要求6213との対応をとる。サービス・ディレクタプロセスを生成して、キャンセル要求6205とキャンセル要求6213とを処理するプロセスを生成する。サービス・ディレクタプロセスは、キャンセル要求6205とキャンセル要求6213の内容を照合して、決済処理機関に対するキャンセル要求6102(9007)として、決済システム103に送信する。

【0985】図93(c)に示すように、キャンセル要求6102は、メッセージがキャンセル要求6102であることを示すヘッダ情報、キャンセル要求ヘッダ6317と、暗号

を復号化した決済完了通知5937と、このキャンセル要求6102の有効期間を示す有効期間6218と、サービス提供者ID6319と、このキャンセル要求6102を発行した日時を示す発行日時6220とから成るデータについて、サービス提供者のデジタル署名を行ない、決済処理機関宛に封鎖化したものである。

【0986】決済システム103は、キャンセル要求6102を受信し、暗号を復号化し、デジタル署名をチェックして、キャンセル処理を行なう。そして、キャンセル完了通知6103(9008)を生成し、サービス提供システム103の決済処理機関プロセスに送信する。

【0987】図93(d)に示すように、キャンセル完了通知6103は、メッセージがキャンセル完了通知6103であることを示すヘッダ情報、キャンセル完了通知ヘッダ6325と、決済システム103が行なったキャンセル処理をユニークに示す番号、キャンセル番号6226と、暗号を復号化したキャンセル要求6221と、決済処理機関のデジタル署名をしたサービス提供者向けキャンセル情報6227と、決済処理機関のデジタル署名をしたマーチャント向けキャンセル情報6328と、決済処理機関のデジタル署名をしたユーザ向けキャンセル情報6329と、決済処理機関ID6230と、この決済完了通知を発行した日時を示す発行日時6331とから成るデータについて、決済処理機関のデジタル署名を行ない、サービス提供者宛に封鎖化したものである。

【0988】サービス提供システム103の決済処理機関プロセスは、キャンセル完了通知6103を受信し、暗号を復号化し、デジタル署名をチェックして、キャンセル完了通知6132をサービス・ディレクタプロセスに送る。サービス・ディレクタプロセスは、キャンセル完了通知6133から、キャンセル完了通知6341とキャンセル処理情報6350とを生成する。マーチャントプロセスは、キャンセル完了通知6341をマーチャント宛に封鎖化し、キャンセル完了通知6104(9009)として、クレジット決済端末300に送信し、ユーザプロセスは、キャンセル処理情報6350を、ユーザ宛に封鎖化し、キャンセル処理情報6105(910)として、パーソナル・クレジット端末100に送信する。

【0989】図93(e)に示すように、キャンセル完了通知6104は、メッセージがキャンセル完了通知6104であることを示すヘッダ情報、キャンセル完了通知ヘッダ6336と、キャンセル番号6337と、暗号を復号化したキャンセル要求6205と、決済処理機関のデジタル署名をしたマーチャント向け決済情報6322と、サービス提供システムにおける処理に関する情報を示すサービス提供者処理情報6328と、サービス提供者ID6329と、このキャンセル完了通知6104を発行した日時を示す発行日時6340とから成るデータについて、サービス提供者のデジタル署名を行ない、マーチャント宛に封鎖化したものである。サービス提供者処理情報6338は、サービス提供者のオプション

かつて規定する情報であり、規定されない場合もある。  
 10.9.9.01 図9.3 (1) に示すように、キャンセル処理  
 履歴情報6105は、キャンセルがキャンセル処理履歴情報  
 05であることを示すペンダ情報、キャンセル処理履歴情  
 報ペンダ6345と、キャンセル理由6346と、番号を識別し  
 たキャンセル理由6343と、決済処理履歴のデジタル署名  
 をしたユーザ向け決済情報6332と、キャンセル処理ステ  
 ュスにおける処理に関する情報と示すキャンセル提供者処理  
 履歴6347と、キャンセル提供先ID6348と、このキャンセ  
 ル処理履歴情報6105を発行した日時を示す発行日時6349と  
 から成るデータについて、キャンセル提供者のデジタル署  
 名を行ない、ユーザ側には提供しないのである。サビー  
 ス提供者処理情報6347は、キャンセル提供者のオプショ  
 ンで規定する情報であり、規定されない場合もある。

【09991】クレジット決済番号1001は、キャンセル料を  
了通知6104を受信し、暗号を復号化し、デジタル署名を  
チェックして、その内容をしC D303に表示する。一  
方、バーチャル・クレジット番号1004は、キャンセル処  
理代償債6105を受信し、暗号を復号化し、デジタル署名  
をチェックして、その内容をしC D303に表示する。

【0992】次に、“顧客サービスコール”の処理において、機器間で交換されるメッセージの内容について説明する。

〔0595〕図94(a)は、「顧客サービスコール」の処理における検索用のメッセージ交換の手順を示し、図95(a)～(e)は、「顧客サービスコール」の処理において、検索間で交換するメッセージの内容を示している。図94(a)は、図45(a)から、検索間で交換するメッセージの部分抜き出した図であり、図94(a)と図45(a)とは、同じ「顧客サービスコール」の処理を示している。

【0994】まず、ケーチャントの担当者が、顧客サービスコール操作(1)210を行なうと、クレジット決済請求サービスコール操作(1)210を生成し、“顧客サービスコール”の処理を開始する。クレジット決済請求サービスコールサービスコール要求(1)210(2)202を生成し、3001は、顧客サービスコール要求(1)210(2)202を生成し、クレジット決済通信で、サービス提供システム102のケーチャントプロセスに送信する。

[illegible]

【0990】 サービス課長シズム1020がマーズン・ト  
ワラセは、顧客サービスコール要求6300を受信し、暗  
号を復号化し、顧客データベースをサーチして、顧客サ  
ービスコール要求6406をサード・マーズン・トワラセに  
送る。サード・マーズン・トワラセは、サービスディ  
レクタワラセを生じ、顧客サービスコール要求64  
06を処理するワラセグループを生じる。サード・マ  
ーズン・トワラセは、顧客サービスコール要求番号に対応  
するユーザを判定し、ユーザのアクセス制御情報と照合  
して、顧客サービスコール番号1111と顧客サービスコー  
ル6406とを生じる。ユーザデータベース  
番号6411を、ユーザ別に封鎖して、顧客サービスコー  
ル6401(1120)として、ユーザのパーソナル・タレツ  
ト編成100に送出し、マーズン・トワラセは、顧客サ  
ービスコール応答6406を、マーズン・トワラセに封鎖化し、  
顧客サービスコール応答6302(1120)として、タレツ  
トの封鎖末300に送出す。

【10011】サービス提供システムは、着信履歴番号003を受信し、暗証番号6333をサーチし、チャリクタブス・デイルクタブロセスは、着出し応答6440を生成し、サーチをサーチタブ類に翻訳し、呼び出し、クレジット決済端末300と接続し、暗号を復号化して、00とバーソナル・クレジット端末となる。

【1003】図95 (d) に示すは、メッセージが着信応答6303で情報、着信履歴番号6430と、クレジット暗証番号6431と、音声が設定した要求番号6431と、音声が成るデータについて、サービスものである。

[illegible]

が、同い合わせコール要求631  
1 D6501と、担当者名6502  
この同い合わせコール要  
発行日時6505とから成るデ  
タル運名を行ない、サービ  
である。担当者名6503は、  
チャントのオプショヨンで設  
けない場合もある。

スデム103のユーザプロセ  
6507を受信し、暗号を復号  
して、同い合わせコール  
ユーザプロセスに送る。サー  
ビス、サービズ、チャレクタ  
ワセコール要求6506を処理す  
る。サービス、チャレクタ

[illegible]

1100431 木、国産、シベリ  
に産せ、404は、マツセージが呼ぶ  
とを示すヘッダ情報、呼び出し足  
ジット法済端来300が設定した要  
ータ暗号鍵6438とから成るデータ  
ト列に料理したものである。  
【1005】音声データ暗号鍵64  
6438は、通話時に、音声データ  
の暗号鍵であり、この音声デー  
・ケジット端来100の音声デー  
721613と、ケジット法済端来

アロセ入は、ローチヤントロ  
間い合わせコール6515と間  
生成する。ローチヤントロ  
6515を、ローチヤントロ  
6307(21110)として、クレ  
ユーザシロセ入は、間い合  
知に封鎖し、間い合わせ  
、バソナル・クレシロセ入  
[1 0 1 1] 図9.6 (b) t  
ール6530は、メッセンジャ  
るに示すバソナル封鎖

顧客アンケートを参照して、  
 合わせてコール応答65秒とを  
 設定せし、問い合わせコール  
 料を無料化し、問い合わせコ  
 ール応答65秒とを、ユーザ  
 へのコール応答65秒(31分)とし  
 て決着額100に返償する。  
 これにより、問い合わせコ  
 ール応答65秒とを、ユーザ  
 へのコール応答65秒(31分)とし  
 て決着額100に返償する。

【0998】図95(c)に示すように、顧客サービスコール応答501は、メッセージが顧客サービスコール応答503であることを示すヘッダ情報、顧客サービスコール応答614と、サービス提供システム102からの応答メッセージ612と、サービス提供者ID614と、この主要受信時刻614と、サービス提供者ID614と、発行日時615とからなるデータに示す、サービス提供者のデジタル署名を行ない、メッセージ頭に封鎖したものである。

シラタタ (GCR[P7]251) などに規定  
 ジュウ・増来100とワシツト決決  
 略号化して音字通語を行なう。こ  
 ない場合は、この音字データ(表  
 11006) 次に、「問い合わせる  
 て、機器間で交換されるメッセ  
 ージ。  
 (11007) 図9.4 (b) は、  
 処理における機器間のメッセー  
 9.6 (a) ~ (e) は、「問いあ

[illegible]

ソナル・クリジント編著(00  
サービス提供者) D6513  
307を発行した日時を示す規  
定について、サービス提供  
ヤーチャント列に對應した  
に示すように、問い合わせコ  
ジが問い合わせコール番63  
情報、問い合わせコール番客  
供システム102からの応答メ

【0999】バザンツト及び特開第3501号は、デジタリ電  
コル伝送系3032を具備し、暗号を復号化し、デジタリ電  
名をチェクシツテ、”呼び出し中”を表示する。  
【1000】バザンツト・ケルジツト編第1001は、顧客  
サードスコル301を愛用し、暗号を復号化し、デジタリ電  
り署名をチェクシツテ、顧客サードスコル301をス  
を生成し、”顧客サードスコル”の処理を開始する。ノ  
ーナル・ケルジツト編第1001は、まず、スビーカから  
ーザが電話機1107を行なうと知らせる。そして、  
コージャを出力して、ユーザに暗号を知らせる。サード  
ジツト編第1001は、暗号伝送系3033(11208)を生成して、サ  
ード提供システム103のユーザプロセッサに送信する。

る。図9.4 (b) は、図4.5 (a) のように、 $\alpha$  の値を大きくするメッセンジの部分抜き出し (b) と図4.5 (b) は、同じ処理を示している。

[1.008] まず、ユーザが、 $\alpha$  の値を行なうと、パーソナル・クォータ、問い合わせコールプロセスは、問い合わせコールプロセスを開始する。パーソナル100は、まず、問い合わせを生成し、デジタル無線電話通信システム100のユーザプロセッサに送付

「問い合わせコール」の  
b) から、機器間で交換  
した図であり、図 9-4  
「問い合わせコール」の  
問い合わせコール動作21  
レジャット決着端未100  
を生成し、「問い合わせ  
コール」要求6307(31215)  
で、サービス提供ジス  
サービス6307を受信し、暗号を  
【01013】パーソナル・  
合わせコール応答6308を受  
タル署名をデエックして、  
【01014】クレジャット決  
ール6307を受信し、暗号を

ル・クレジツトは、防弾丸100  
、サービス提供者1 D6522  
、客室6303を発行した日時を示  
すデータについて、サービス提  
供、ユーザ宛に封鎖化したも  
の。

【1000】図96 (a) に示すように、問い合わせコール要求63070は、メッセージが問い合わせコール要求63070であることを示すヘッダ情報、問い合わせコール要求63070の識別子ID65010と、担当者名65030と、この問い合わせコール要求をユーザに示す要求番号65030と、ユーザID65040と、この問い合わせコール要求63070を発行した日時を示す発行日時65050とから成るデータについて、ユーザのデジタル署名を行ない、サブキーを用いて、ユーザのデジタル署名を行ない、サブキーを用いて封鎖化し、メッセージのオブジェクトで規定する情報であり、規定された場合もある。

[illegible]

フロセス又は、サーチエンジンの顧客テーブルを参照して、  
 問い合わせコード6515と問い合わせコード6524とを  
 生成する。サーチエンジンテーブル又は、問い合わせコード  
 6515を、サーチエンジン宛に封書化し、問い合わせコード  
 6307(1216)として、ケーブルネットワーク未300に送信し、  
 ユーザーフロセスは、問い合わせコード6524をユーザ

列に封鎖化し、問い合わせコール応答308(21217)として、パーソナル・クルジツト決済端末100に送信する。  
【1011】図96(b)に示すように、問い合わせコール6301は、メッセージが問い合わせコール6307であることを示すヘッダ情報、問い合わせコールヘッダ6510

と、顧客番号6511と、バーソナル・クルシット顧客100と、顧客番号6511と、サービエ提供番号1 D6513が規定した要求番号6512と、サービエ提供した日時を示すこの間い合わせコール6301を履行した日時について、サービエ提供行日時6514とから成るデータについて、サービエ提供のデジタル署名を行ない、マージヤント宛に封書化しものである。

[1012] 図96(c)に示すように、問い合わせコードが56308は、マッテージ間い合わせコールが508であることを示すマッテージ情報、問い合わせコールが56519と、サーチと掘上げシステム102からのお客様ヘンダ5519と、サーチと掘上げ従業員1 D6522が設定した要求番号551と、サーチと掘上げ日時を、この間い合わせコールが56308を発行して日時をす発行日時553とから成るデータに対して、サーチした供者の日付タル番号を行ない、ユーザ間に封鎖化するのである。

【10113】バーソナル・クレジット額米100は、問い合わせ必答6308を受領し、暗号を復号化し、デジタル署名をチェツクして、“平出し中”を提示する【10114】クレジット決済額米100は、問い合わせメール6307を受領し、暗号を復号化し、デジタル署名を

エックして、問い合わせコールプロセスを生成し、「問い合わせコール」の処理を開始する。クレジット決済端末300は、まず、スピーカから着信音を出力して、マーチャントに着信を知らせる。そして、マーチャントが通話操作120を行なうと、クレジット決済端末300は、着信応答6309(2121)を生成して、サービス提供システム102のマーチャントプロセスに送信する。

[1015] サービス提供システム102のマーチャントプロセスは、着信応答6309を受信し、暗号を復号化して、着信応答6531をサービス・ディレクタプロセスに送る。サービス・ディレクタプロセスは、着信応答6531から、呼び出し応答6538を生成し、ユーザプロセスが、これをユーザ宛に封書化し、呼び出し応答6310(2122)として、パーソナル・クレジット端末100に送信する。

[1016] パーソナル・クレジット端末100は、呼び出し応答6310を受信し、暗号を復号化して、パーソナル・クレジット端末100とクレジット決済端末300とは音声通話状態となる。

[1017] 図9(d)に示すように、着信応答6309は、メッセージが着信応答6309であることを示すヘッダ情報、着信応答ヘッダ6528と、パーソナル・クレジット決済端末100が設定した要求番号6529と、音声データ暗号6530とから成るデータについて、サービス提供者宛に封書化したものである。

[1018] また、図9(e)に示すように、呼び出し応答6310は、メッセージが呼び出し応答6310であることを示すヘッダ情報、呼び出し応答ヘッダ6535と、パーソナル・クレジット決済端末100が設定した要求番号6536と、音声データ暗号6537とから成るデータについて、ユーザ宛に封書化したものである。

[1019] 音声データ暗号6530と音声データ暗号6537は、音声通話時に、音声データを暗号化するための共通の暗号であり、この音声データ暗号は、パーソナル・クレジット端末100の音声データ暗号レジスタ(CRYP7)21613と、クレジット決済端末300の音声データ暗号レジスタ(CRYP7)22611に設定して、パーソナル・クレジット端末100とクレジット決済端末300とは音声データを暗号化して音声通話を行なう。音声データの暗号化をしない場合には、この音声データ暗号は設定されない。

[1020] 次に、セッション確立処理、リモートアクセス処理、データアップロード処理、強制のデータアップロード処理、データバックアップ処理、「決済」の処理、「キャンセル」の処理、「顧客サービスコール」の処理、及び「問い合わせコール」の処理の各処理における、パーソナル・クレジット端末100、クレジット決済端末300、決済システム103、並びに、サービス提供システム102のサービス・マネージャプロセス、サービス・ディレクタプロセス、ユーザプロセス、マーチャントプロセス、及び決済処理機関プロセスの各プロセスが行な

う処理の詳細について説明する。  
[1021] パーソナル・クレジット端末、及びクレジット決済端末の全体的な処理フローについては、それぞれ、図51、及び図61の説明において述べた通りである。パーソナル・クレジット端末、及び、クレジット決済端末は、セッション確立処理、リモートアクセス処理、データアップロード処理、強制のデータアップロード処理、データバックアップ処理、「決済」の処理、「キャンセル」の処理、「顧客サービスコール」の処理、及び「問い合わせコール」の処理の各処理に対応するプロセスを、それぞれ、プロセスリストに登録し、メインルーチンの各プロセスの処理によって、各処理を実行する。

[1022] それに対して、サービス提供システムは、サービス・マネージャプロセス、サービス・ディレクタプロセス、ユーザプロセス、マーチャントプロセス、及び決済処理機関プロセスの5種類のプロセスの連携処理によって、各処理を実行する。

[1023] 5種類のプロセスの内、まず、サービス・マネージャプロセスは、図97から図98に示す処理フローにしたがって、サービス・ディレクタプロセス、ユーザプロセス、マーチャントプロセス、決済処理機関プロセスといった他のプロセスを管理する。

[1024] サービス・マネージャプロセスは、常に起動していて、通常、ステップ6600で、パーソナル・クレジット端末、または、クレジット決済端末からの着呼要求のメッセージ、及び、各プロセスからのメッセージを待っている。サービス・マネージャプロセスは、メッセージを受信すると、ステップ6601〜ステップ6618、及び、ステップ6700〜6709に示す、メッセージの種類に応じた処理を行なう。また、ステップ6600に戻る。

[1025] サービス・マネージャプロセスは、メッセージが着呼要求であった場合は、ステップ6605で、呼び出し応答をユーザプロセス、または、マーチャントプロセスを生成するプロセス生成処理を行なう。

[1026] また、メッセージがマーチャントプロセスからの信用照会要求であった場合には、サービス・マネージャプロセスは、まず、ステップ6607で、メッセージリスト4405に、受信した信用照会要求に対応する支払要求が登録されているかを調べ、登録されていない場合には、ステップ6608で、受信したメッセージをメッセージリストに登録し、登録されている場合には、ステップ6609で、サービス・ディレクタプロセスを生成して、サービス・ディレクタプロセスと、ユーザプロセスと、マーチャントプロセスとによるプロセスグループを生成し、ステップ6610で、登録されていたメッセージをメッセージリストから削除して、ステップ6611で、サービス・ディレクタプロセスに信用照会要求と支払要求とを送信する。

[1027] また、メッセージがユーザプロセスからの

支払要求であった場合には、サービス・マネージャプロセスは、まず、ステップ6612で、メッセージリスト4405に、受信した支払要求に対応する信用照会要求が登録されているかを調べ、登録されていない場合には、ステップ6613で、受信したメッセージをメッセージリストに登録し、登録されている場合には、ステップ6609へ進み、メッセージが信用照会要求であった場合と同様の処理を行なう。

[1028] また、メッセージがマーチャントプロセスからのキャンセル要求であった場合には、サービス・マネージャプロセスは、まず、ステップ6614で、メッセージリスト4405に、受信したキャンセル要求に対応するユーザプロセスからのキャンセル要求が登録されているかを調べ、登録されていない場合には、ステップ6615で、受信したメッセージをメッセージリストに登録し、登録されている場合には、ステップ6616で、サービス・ディレクタプロセスを生成して、サービス・ディレクタプロセスと、ユーザプロセスと、マーチャントプロセスとによるプロセスグループを生成し、ステップ6617で、登録されていたメッセージをメッセージリストから削除して、ステップ6618で、サービス・ディレクタプロセスに、マーチャントプロセスからのキャンセル要求とユーザプロセスからのキャンセル要求とを送信する。

[1029] また、メッセージがユーザプロセスからのキャンセル要求であった場合には、サービス・マネージャプロセスは、まず、ステップ6619で、メッセージリスト4405に、受信したキャンセル要求に対応するマーチャントプロセスからのキャンセル要求が登録されているかを調べ、登録されていない場合には、ステップ6620で、受信したメッセージをメッセージリストに登録し、登録されている場合には、ステップ6616へ進み、メッセージがマーチャントプロセスからのキャンセル要求であった場合と、同様の処理を行なう。

[1030] ステップ6608、ステップ6613、ステップ6616、及びステップ6620における受信したメッセージのメッセージリストへの登録では、メッセージに含まれるマーチャントID、トランザクション番号、及び要求番号から、照合データを生成して、メッセージをメッセージリストに登録する。

[1031] また、ステップ6609及びステップ6616におけるプロセスグループの生成では、まず、サービス・ディレクタプロセスを生成して、プロセスグループ管理情報、及び、サービス・ディレクタプロセス管理情報を登録し、さらに、ユーザプロセス管理情報、及び、マーチャントプロセス管理情報を更新して、サービス・ディレクタプロセスと、ユーザプロセスと、マーチャントプロセスとによるプロセスグループを生成する。

[1032] また、メッセージがマーチャントプロセスからの顧客サービスコール要求であった場合には、サービス・マネージャプロセスは、ステップ6704で、サービ

ス・ディレクタプロセスを生成して、サービス・ディレクタプロセスと、マーチャントプロセスとによるプロセスグループを生成し、ステップ6705で、サービス・ディレクタプロセスに顧客サービスコール要求を送信する。  
[1033] ステップ6704のプロセスグループの生成では、まず、サービス・ディレクタプロセスを生成して、プロセスグループ管理情報、及び、サービス・ディレクタプロセス管理情報を登録し、さらに、マーチャントプロセス管理情報を更新して、サービス・ディレクタプロセスと、マーチャントプロセスとによるプロセスグループを生成する。

[1034] また、メッセージがユーザプロセスからの問い合わせコール要求であった場合には、サービス・マネージャプロセスは、ステップ6706で、サービス・ディレクタプロセスを生成して、サービス・ディレクタプロセスと、ユーザプロセスとによるプロセスグループを生成し、ステップ6707で、サービス・ディレクタプロセスに問い合わせコール要求を送信する。

[1035] ステップ6706のプロセスグループの生成では、まず、サービス・ディレクタプロセスを生成して、プロセスグループ管理情報、及び、サービス・ディレクタプロセス管理情報を登録し、さらに、ユーザプロセス管理情報を更新して、サービス・ディレクタプロセスと、ユーザプロセスとによるプロセスグループを生成する。

[1036] また、メッセージがサービス・ディレクタプロセスからのメンバープロセス要求であった場合には、サービス・マネージャプロセスは、ステップ6708で、要求されたプロセスを、サービス・ディレクタプロセスのプロセスグループに追加するメンバープロセス生成処理を行なう。この際、必要に応じて、サービス・マネージャプロセスは、要求されたプロセスを生成する。

[1037] また、メッセージがプロセス消去要求であった場合には、サービス・マネージャプロセスは、ステップ6709で、要求されたプロセスを消去するプロセス消去処理を行なう。この際、必要に応じて、サービス・マネージャプロセスは、各プロセスのプロセス管理情報、及び、プロセスグループ管理情報4404、並びにメッセージリスト4405を更新する。

[1038] また、ステップ6605のプロセス生成処理は、図99に示す処理フローにしたがって行なわれる。  
[1039] サービス・マネージャプロセスは、まず、ステップ6800で、着呼要求の中に含まれる呼び出しの電話番号と、ユーザリスト4300のユーザ電話番号、及び、マーチャントリスト4301のマーチャント電話番号と、照合して、要求者を判定する。電話番号情報が、ユーザ電話番号と一致した場合には、要求者はユーザであると判定して、ステップ6801へ進み、マーチャント電話番号と一致した場合には、要求者はマーチャントであると判定して、ステップ6804へ進み、いずれにも一致しな

った場合には、ユーザ、または、マニファストからの着呼要求ではないと判断して、プロセスを生成せずに、プロセスを生成処理を終了する。

【1040】 ステップ6601では、登録されているユーザプロセスを管理情報を調べ、要求者であるユーザに対処するユーザプロセスが、既に、存在していないかを判定する。ユーザプロセスが存在していない場合には、ステップ6602へ進み、ユーザプロセスを生成し、ユーザプロセスを管理情報を登録して、プロセス生成処理を終了する。また、ユーザプロセスが既に存在している場合には、ユーザへの成りすまし等の不正行為が行われている可能性があるので、ステップ6603へ進み、管理システムにエラーメッセージを送信して、プロセス生成処理を終了する。

【1041】 ステップ6604では、登録されているマニファストプロセスを管理情報を調べ、要求者であるマニファストに対処するマニファストプロセスが、既に、存在していないかを判定する。マニファストプロセスが存在していない場合には、ステップ6605へ進み、マニファストプロセスを生成し、マニファストプロセスを管理情報を登録して、プロセス生成処理を終了する。また、マニファストプロセスが既に存在している場合には、マニファストへの成りすまし等の不正行為が行われている可能性があるので、ステップ6606へ進み、管理システムにエラーメッセージを送信して、プロセス生成処理を終了する。

【1042】 次に、ユーザプロセスは、図100に示す処理フローにしたがって、マニファスト・クレジット端末からのメッセージ、及び、マニファスト・デイレクタプロセスからのメッセージに応じた処理を行なう。

【1043】 サービス・マニファストプロセスによって生成されたユーザプロセスは、まず、ステップ6900で、マニファスト・クレジット端末とのセッション確立処理を行ない、ステップ6901とステップ6905とで、マニファスト・クレジット端末またはマニファスト・デイレクタプロセスからのメッセージを受け、ステップ6901では、メッセージ受信の判定を行ない、ステップ6905では、タイムアウトの判定を行なう。

【1044】 メッセージを受信した場合、ユーザプロセスは、ステップ6902で、ユーザプロセスのメッセージ・ステータスを“アクティブ”状態に変更し、ステップ6903で、受信したメッセージに応じた処理を行なう。例えば、マニファスト・クレジット端末から“支払要求”を受信した場合には、ステップ6903で、ユーザプロセスにおける“決済”の処理を行なう。ステップ6903の処理を終了すると、ユーザプロセスは、ステップ6904で、プロセス・ステータスを“アイドル”状態に変更して、ステップ6901に戻る。

【1045】 ステップ6905のタイムアウトの判定では、タイムアウト時間T<sub>NOU</sub> (T<sub>NOU</sub> >0) 以上の間、新たな

メッセージを受信しない場合、ユーザプロセスはタイムアウトして、ステップ6906で、ユーザプロセス・タイムアウト処理を行なう。ユーザプロセス・タイムアウト処理によって、ユーザプロセスは、サービス・マニファストプロセスによって消去され、ユーザプロセスとマニファスト・クレジット端末との間の回線は切断される。

【1046】 つまり、ユーザプロセスは、タイムアウト時間T<sub>NOU</sub>以上の間、マニファスト・クレジット端末、または、サービス・デイレクタプロセスから、新たなメッセージを受信しない場合、自動的に消去され、マニファスト・クレジット端末との間の回線は切断される。

【1047】 次に、マニファストプロセスは、図101に示す処理フローにしたがって、クレジット決済端末からのメッセージ、及び、サービス・デイレクタプロセスからのメッセージに応じた処理を行なう。

【1048】 サービス・マニファストプロセスによって生成されたマニファストプロセスは、ユーザプロセスの場合と同様に、まず、ステップ7000で、クレジット決済端末とのセッション確立処理を行ない、ステップ7001とステップ7005とで、クレジット決済端末、または、サービス・デイレクタプロセスからのメッセージを受け、ステップ7001では、メッセージ受信の判定を行ない、ステップ7005では、タイムアウトの判定を行なう。

【1049】 メッセージを受信した場合、マニファストプロセスは、ステップ7001で、マニファスト・クレジットプロセス・ステータスを“アクティブ”状態に変更し、ステップ7003で、受信したメッセージに応じた処理を行なう。例えば、クレジット決済端末から“借入照会要求”を受信した場合には、ステップ7004で、マニファストプロセスにおける“決済”の処理を行なう。ステップ7004で、プロセス・ステータスを“アイドル”状態に変更して、ステップ7001に戻る。

【1050】 ステップ7005のタイムアウトの判定では、タイムアウト時間T<sub>NOU</sub> (T<sub>NOU</sub> >0) 以上の間、新たなメッセージを受信しない場合、マニファストプロセスは、メッセージを受信しない場合、自動的に消去され、クレジット決済端末との間の回線は切断される。

【1051】 つまり、マニファストプロセスは、タイムアウト時間T<sub>NOU</sub>以上の間、クレジット決済端末、または、サービス・デイレクタプロセスから、新たなメッセージを受信しない場合、自動的に消去され、クレジット決済端末との間の回線は切断される。

【1052】 次に、決済処理間プロセスは、図102に示す処理フローにしたがって、決済システムからのメッセージ、及び、サービス・デイレクタプロセスからの

メッセージに応じた処理を行なう。

【1053】 サービス・マニファストプロセスによって生成された決済処理間プロセスは、まず、ステップ7100で、決済システムとの通信回線の初期化処理を行ない、ステップ7101とステップ7105とで、決済システム、または、サービス・デイレクタプロセスからのメッセージを受け、ステップ7101では、メッセージ受信の判定を行ない、ステップ7105では、タイムアウトの判定を行なう。

【1054】 メッセージを受信した場合、決済処理間プロセスは、ステップ7102で、決済処理間プロセスのメッセージ・ステータスを“アクティブ”状態に変更し、ステップ7103で、受信したメッセージに応じた処理を行なう。例えば、サービス・デイレクタプロセスから“決済要求”を受信した場合には、ステップ7103で、決済処理間プロセスにおける“決済”の処理を行なう。ステップ7103の処理を終了すると、決済処理間プロセスは、ステップ7104で、プロセス・ステータスを“アイドル”状態に変更して、ステップ7101に戻る。

【1055】 ステップ7105のタイムアウトの判定では、タイムアウト時間T<sub>NTPT</sub> (T<sub>NTPT</sub> >0) 以上の間、新たなメッセージを受信しない場合、決済処理間プロセスはタイムアウトして、ステップ7106で、決済処理間プロセス・タイムアウト処理を行なう。決済処理間プロセス・タイムアウト処理によって、決済処理間プロセスは、サービス・マニファストプロセスによって消去され、決済処理間プロセスと決済システムとの間の回線は切断される。

【1056】 つまり、決済処理間プロセスは、タイムアウト時間T<sub>NTPT</sub>以上の間、決済システム、または、サービス・デイレクタプロセスから、新たなメッセージを受信しない場合、自動的に消去され、決済システムとの間の回線は切断される。

【1057】 また、ユーザプロセスとマニファスト・クレジット端末100との間の通信費用が、通信回線の使用時に依存する場合には、タイムアウト時間T<sub>NOU</sub>は、通信料金の体系に依存した値となる。例えば、通信回線の使用時間に対して、段階的に課金される場合には、タイムアウト時間T<sub>NOU</sub>は、一定時間T<sub>NOU0</sub> (T<sub>NOU0</sub> >0) 以上で、かつ、次の通信料金の変化点を越えたい最大の値となる。この場合は、マニファスト・クレジット端末と、ユーザプロセスとの通信回線は、通信費用が増加しない範囲で、できる限り長い時間の間接続される。また、通信回線の使用時間に対して、リニアに課金される場合には、タイムアウト時間T<sub>NOU</sub>は、一定時間T<sub>NOU0</sub>となる。

【1058】 同様に、マニファストプロセスとクレジット決済端末100、または、決済処理間プロセスと決済システム103との間の通信費用が、通信回線の使用時間に依存する場合には、ユーザプロセスのタイムアウト時

間T<sub>NOU</sub>の場合と同様に、タイムアウト時間T<sub>NOU</sub>、T<sub>NTPT</sub>は、それぞれ通信料金の体系に依存した値となる。

【1059】 サービス・デイレクタプロセスについては、この後の“決済”、“キャンセル”、“顧客サービスコール”、“問い合わせコール”の処理の各処理における説明において詳しく述べる。また、決済システムについては、“決済”、“キャンセル”の処理の各処理における説明において詳しく述べる。

【1060】 次に、マニファスト・クレジット端末から、ユーザプロセスに接続するセッション確立処理における処理フローについて説明する。

【1061】 図103と、図104は、それぞれ、マニファスト・クレジット端末からユーザプロセスに接続する場合のセッション確立処理におけるマニファスト・クレジット端末のセッション確立プロセスと、ユーザプロセスとの処理フローを示している。

【1062】 まず、マニファスト・クレジット端末は、ステップ7200で、デジタル公衆網へ発呼要求4500を送信。及び、デジタル公衆網へ発呼要求4500を受信して、ユーザプロセスとの回線を接続する。この時、サービス・マニファストプロセスは、デジタル公衆網から発呼要求4500を受信し、ステップ6000のプロセス生成処理でユーザプロセスを生成する。生成されたユーザプロセスは、ステップ7300で、デジタル公衆網へ発呼要求4500を送信して、マニファスト・クレジット端末との回線を接続する。

次に、ユーザプロセスは、ステップ7301で、テストパターンA700を生成し、ステップ7302で、テストパターンAをユーザの公開鍵で暗号化して、暗証テストA4506を生成し、ステップ7303で、暗証テストAをマニファスト・クレジット端末に送信する。

【1063】 一方、マニファスト・クレジット端末は、ステップ7201で、テストパターンB4405を生成し、ステップ7202で、テストパターンBをサービス提供者の公開鍵で暗号化して暗証テストBを生成し、ステップ7203とステップ7211とで、ユーザプロセスから暗証テストAを受信するのを待っている。ステップ7203では、暗証テストAの受信の判定を行ない、ステップ7211では、タイムアウトの判定を行なう。

【1064】 ステップ7211のタイムアウトの判定では、タイムアウト時間T<sub>TAU</sub> (T<sub>TAU</sub> >0) 以上の間、暗証テストAを受信しない場合、マニファスト・クレジット端末はタイムアウトして、ステップ7312で、LCDにエラーメッセージを表示し、さらに、ステップ7313で、回線を切断して、セッション確立処理を終了する。

【1065】 暗証テストAを受信した場合には、マニファスト・クレジット端末は、ステップ7304で、暗号化されたテストパターンAをユーザのプライベート鍵で復号化したテストパターンAとから、暗証テストA4507を生成し、ステップ7307で、暗証テストA4507をユーザプロ

セスに送信する。

【1066】 認証テストAをパーソナル・クレジット端末に送信したユーザプロセスは、ステップ7304とステップ7312とで、パーソナル・クレジット端末から、認証テストA応答を受信するのを待っている。ステップ7304では、認証テストA応答の受信の判定を行ない、ステップ7312では、タイムアウトの判定を行なう。

【1067】 ステップ7313のタイムアウトの判定では、タイムアウト時間TTMO (TTMO 0) 以上の間、認証テストA応答を受信しない場合、ユーザプロセスはタイムアウトして、ステップ7313で、セッション確立エラー処理を行ない、セッション確立処理を終了する。セッション確立エラー処理によって、ユーザプロセスは、サービス・マネージャプロセスによって消去され、回線は切斷される。

【1068】 認証テストA応答を受信した場合、ユーザプロセスは、ステップ7305で、送信した認証テストAのテストパターンAと、受信した認証テストA応答のテストパターンAとを照合して、パターンが一致した場合には、ユーザの認証に失敗したと判定して、ステップ7314で、セッション確立エラー処理を行ない、セッション確立処理を終了する。

【1069】 ユーザプロセスは、ステップ7305で、暗号化されたテストパターンBをサービス提供者のプライベート鍵で復号化し、ステップ7307で、セッション許可メッセージ7308で、セッション許可メッセージをユーザの公開鍵で暗号化して、暗号化されたテストパターンBと、暗号化したセッション許可メッセージとから認証テストB応答4508を生成し、ステップ7309で、認証テストB応答をパーソナル・クレジット端末に送信する。そして、ステップ7310で、ユーザ・ステイタスをセッション確立状態に変更し、ステップ7311で、プロセス・ステイタスを "アイドル" 状態に変更して、セッション確立処理を終了し、ユーザプロセスは、図100におけるステップ6901へと進む。

【1070】 認証テストA応答をユーザプロセスに送信したパーソナル・クレジット端末は、ステップ7207とステップ7214とで、ユーザプロセスから、認証テストB応答を受信するのを待っている。ステップ7207では、認証テストB応答の受信の判定を行ない、ステップ7214では、タイムアウトの判定を行なう。

【1071】 ステップ7214のタイムアウトの判定では、タイムアウト時間TTMO (TTMO 0) 以上の間、認証テストB応答を受信しない場合、パーソナル・クレジット端末はタイムアウトして、ステップ7215で、LCDにエラーメッセージを表示し、さらに、ステップ7216で、回線を切斷して、セッション確立処理を終了する。認証テストB応答を受信した場合、パーソナル・クレジット端末は、ステップ7208で、送信した認証テストBのテスト

トパターンBと、受信した認証テストB応答のテストパターンBとを照合して、パターンが一致した場合には、ステップ7209へ進み、一致しなかった場合には、サービス提供者の認証に失敗したと判定して、ステップ7217で、LCDにエラーメッセージを表示し、さらに、ステップ7218で、回線を切斷して、セッション確立処理を終了する。

【1072】 パーソナル・クレジット端末は、ステップ7209で、暗号化されたセッション許可メッセージをユーザのプライベート鍵で復号化し、ステップ7210で、パーソナル・ステイタスをセッション確立状態に変更して、セッション確立処理を終了する。

【1073】 クレジット決済端末から、マーチャントプロセスに接続する場合のセッション確立処理は、パーソナル・クレジット端末から、ユーザプロセスに接続する場合のセッション確立処理と同様の処理を行なう。図105と、図106は、それぞれ、クレジット決済端末からマーチャントプロセスに接続する場合のセッション確立処理における、クレジット決済端末のセッション確立プロセスと、マーチャントプロセスとの処理フローを示している。

【1074】 まず、クレジット決済端末は、ステップ7400で、デジタル公衆網へ発呼要求4800を送信、及び、デジタル公衆網から発呼応答4804を受信して、マーチャントプロセスとの回線を接続する。この時、サービス・マネージャプロセスは、デジタル公衆網から発呼要求4801を受信し、ステップ6806のプロセス生成処理でマーチャントプロセスを生成する。生成されたマーチャントプロセスは、ステップ7600で、デジタル公衆網へ発呼応答4803を送信して、クレジット決済端末との回線を接続する。次に、マーチャントプロセスは、ステップ7501で、テストパターンA5001を生成し、ステップ7502で、テストパターンAをマーチャントプロセスの公開鍵で暗号化して、認証テストA4806を生成し、ステップ7503で、認証テストAをクレジット決済端末に送信する。

【1075】 一方、クレジット決済端末は、ステップ7401で、テストパターンB5005を生成し、ステップ7402で、テストパターンBをサービス提供者の公開鍵で暗号化して、認証テストBを生成し、ステップ7403とステップ7411とで、マーチャントプロセスから認証テストAを受信するのを待っている。ステップ7403では、認証テストAの受信の判定を行ない、ステップ7411では、タイムアウトの判定を行なう。

【1076】 ステップ7411のタイムアウトの判定では、タイムアウト時間TTMO (TTMO 0) 以上の間、認証テストAを受信しない場合、クレジット決済端末はタイムアウトして、ステップ7412で、LCDにエラーメッセージを表示し、さらに、ステップ7413で、回線を切斷して、セッション確立処理を終了する。

【1077】 認証テストAを受信した場合には、クレジ

ット決済端末は、ステップ7404で、暗号化されたテストパターンAをマーチャントのプライベート鍵で復号化し、ステップ7405で、認証テストBと、暗号を復号化したテストパターンAから、認証テストA応答4807を生成し、ステップ7408で、送信した認証テストB応答のテストパターンBと、受信した認証テストB応答のテストパターンBとを照合して、パターンが一致した場合には、サービス提供者の認証に失敗したと判定して、ステップ7417で、LCDにエラーメッセージを表示し、さらに、ステップ7418で、回線を切斷して、セッション確立処理を終了する。

【1078】 認証テストAをクレジット決済端末に送信したマーチャントプロセスは、ステップ7504とステップ7512とで、クレジット決済端末から、認証テストA応答を受信するのを待っている。ステップ7504では、認証テストA応答の受信の判定を行ない、ステップ7512では、タイムアウトの判定を行なう。

【1079】 ステップ7512のタイムアウトの判定では、タイムアウト時間TTMO (TTMO 0) 以上の間、認証テストA応答を受信しない場合、マーチャントプロセスはタイムアウトして、ステップ7513で、セッション確立エラー処理を行ない、セッション確立処理を終了する。セッション確立エラー処理によって、マーチャントプロセスは、サービス・マネージャプロセスによって消去され、回線は切斷される。

【1080】 認証テストA応答を受信した場合には、マーチャントプロセスは、ステップ7505で、送信した認証テストAのテストパターンAと、受信した認証テストA応答のテストパターンAとを照合して、パターンが一致した場合には、マーチャントプロセスの認証に失敗したと判定して、ステップ7514で、セッション確立エラー処理を行ない、セッション確立処理を終了する。

【1081】 マーチャントプロセスは、ステップ7508で、暗号化されたテストパターンBをサービス提供者のプライベート鍵で復号化し、ステップ7507で、セッション許可メッセージ7509を生成し、ステップ7508で、セッション許可メッセージをマーチャントプロセスの公開鍵で暗号化して、暗号化されたテストパターンBと、暗号化したセッション許可メッセージとから認証テストB応答4808を生成し、ステップ7509で、認証テストB応答をクレジット決済端末に送信する。そして、ステップ7510で、マーチャント・ステイタスをセッション確立状態に変更し、ステップ7511で、プロセス・ステイタスを "アイドル" 状態に変更して、セッション確立処理を終了し、マーチャントプロセスは、図101におけるステップ7001へと進む。認証テストA応答をマーチャントプロセスに送信したクレジット決済端末は、ステップ7407とステップ7414とで、マーチャントプロセスから、認証テストB応答を受信するのを待っている。ステップ7407では、認証テストB応答の受信の判定を行ない、ステップ7414では、タイムアウトの判定を行なう。

【1082】 ステップ7414のタイムアウトの判定では、タイムアウト時間TTMO (TTMO 0) 以上の間、認証テストB応答を受信しない場合、ユーザプロセスはタイムアウトして、ステップ7613で、セッション確立エラー処理を

タイムアウトして、ステップ7415で、LCDにエラーメッセージを表示し、さらに、ステップ7416で、回線を切斷して、セッション確立処理を終了する。

【1083】 認証テストB応答を受信した場合、クレジット決済端末は、ステップ7408で、送信した認証テストBのテストパターンBと、受信した認証テストB応答のテストパターンBとを照合して、パターンが一致した場合には、サービス提供者の認証に失敗したと判定して、ステップ7417で、LCDにエラーメッセージを表示し、さらに、ステップ7418で、回線を切斷して、セッション確立処理を終了する。

【1084】 クレジット決済端末は、ステップ7409で、暗号化されたセッション許可メッセージをマーチャントのプライベート鍵で復号化し、ステップ7410で、パーソナル・ステイタスをセッション確立状態に変更して、セッション確立処理を終了する。

【1085】 次に、ユーザプロセスから、パーソナル・クレジット端末に接続する場合のセッション確立処理における処理フローについて説明する。

【1086】 図107と、図108は、それぞれ、ユーザプロセスからパーソナル・クレジット端末に接続する場合のセッション確立処理におけるユーザプロセスと、パーソナル・クレジット端末のセッション確立プロセスとの処理フローを示している。

【1087】 サービス・マネージャプロセスによって生成されたユーザプロセスは、まず、ステップ7600で、デジタル公衆網へ発呼要求4601を送信、及び、デジタル公衆網から発呼応答4604を受信して、パーソナル・クレジット端末との回線を接続する。この時、パーソナル・クレジット端末は、ステップ7700で、デジタル公衆網から発呼要求4602を受信、及び、デジタル公衆網へ発呼応答4603を送信して、ユーザプロセスとの回線を接続する。さらに、パーソナル・クレジット端末は、ステップ7701で、テストパターンC4712を生成し、ステップ7702で、テストパターンCをサービス提供者の公開鍵で暗号化して、認証テストC4806を生成し、ステップ7703で、認証テストCをユーザプロセスに送信する。

【1088】 一方、ユーザプロセスは、ステップ7601で、テストパターンD4716を生成し、ステップ7602で、テストパターンDをユーザの公開鍵で暗号化して、認証テストDを生成し、ステップ7603とステップ7612とで、パーソナル・クレジット端末から、認証テストCを受信するのを待っている。ステップ7603では、認証テストCの受信の判定を行ない、ステップ7612では、タイムアウトの判定を行なう。

【1089】 ステップ7612のタイムアウトの判定では、タイムアウト時間TTMO (TTMO 0) 以上の間、認証テストCを受信しない場合、ユーザプロセスはタイムアウトして、ステップ7613で、セッション確立エラー処理を





エラーメッセージを送信し、ユーザプロセスとのセッションと回線を切断し、LCDに、タイムアウト・エラーを表示する。

〔1117〕リモートアクセスデータを受信した場合、パーソナル・クレジット決済端末は、ステップ8005で、ユーザのプライバシー・レベルを、リモートアクセスデータの暗号を復号化し、ステップ8006で、ユーザが有効なメッセージを行ない、リモートアクセスデータの有効性を検証する。

〔1118〕ユーザが有効なメッセージにパスした場合に、パーソナル・クレジット決済端末は、ステップ8007で、リモートアクセスデータのデータ5009の部分RAMのアドレス情報を、データ5009を格納したローカルアドレスに更新し、ステップ8009で、RAMに格納したデータにアクセスする。そして、ステップ8010で、テンポラリ領域の空き容量から、データアップロード処理が必要か否かを判定し、テンポラリ領域の空き容量が、設定値AU(AU>0)以上ある場合には、そのまま、リモートアクセス処理を終了し、ユーザプロセスを生成し、データアップロード処理へ進む。

〔1119〕ユーザが有効なメッセージにフェイルした場合に、パーソナル・クレジット決済端末は、ステップ8013で、ユーザ・セッション・エラー処理を行ない、リモートアクセス処理を終了する。ユーザ・セッション・エラー処理では、パーソナル・クレジット決済端末は、サービス・提供システム・ユーザプロセスにユーザ・セッション・エラーメッセージを送信し、ユーザプロセスとのセッションと回線を切断し、LCDに、セッション・エラーを表示する。

〔1120〕また、ユーザが有効なメッセージは、サービス・提供システム・ユーザプロセスから受信したメッセージの有効性を検証する処理であり、図111(b)に示すように、ユーザが有効なメッセージは、3種類の検証を行なう。まず、ステップ8014で、サービス提供者IDの署名を検証し、ステップ8015で、サービス提供者IDの署名を照合し、さらに、ステップ8016で、受信したメッセージの発行時刻を検証する。ステップ8016の発行時刻の検証では、受信した情報の発行時刻と現在の時刻とのズレを検証し、ズレが時間TU(TU>0)以上である場合に、サービス提供者のデジタル署名の検証にパスし、サービス提供者IDが一一致し、発行時刻の検証にパスした場合のみ、ユーザが有効なメッセージにパスしたと判定し、それ以外の場合はフェイルしたと判定する。

〔1121〕一方、ユーザプロセスでは、リモートアクセス処理は、リモートアクセス要求5100を受信することによって開始される。ユーザプロセスは、まず、ステップ8100で、サービス提供者のプライバシー・レベルを、受信したリモートアクセス要求の暗号を復号化し、ステップ81

01で、ユーザプロセスが有効なメッセージを行ない、リモートアクセス要求の有効性を検証する。

〔1122〕ユーザプロセスが有効なメッセージにパスした場合には、ユーザプロセスは、ステップ8103で、生成したリモートアクセスデータ5101を生成し、ステップ8103で、生成したリモートアクセスデータをパーソナル・クレジット決済端末に送信して、リモートアクセス処理を終了する。

〔1123〕ユーザプロセスが有効なメッセージにフェイルした場合には、ユーザプロセスは、受信したメッセージは有効ではないと判定し、ステップ8104で、ユーザプロセス・セッション・エラー処理を行ない、リモートアクセス処理を終了する。ユーザプロセス・セッション・エラー処理によって、ユーザプロセスは、サービス・マネージャプロセスによって消去され、パーソナル・クレジット端末とのセッションと回線は切断される。この際、ユーザプロセスは、無効なメッセージを受信したことを示すセッション・エラーメッセージを、管理システム407に送信する。

〔1124〕また、ユーザプロセスが有効なメッセージは、パーソナル・クレジット端末から受信した情報の有効性を検証する処理であり、図112(b)に示すように、ユーザプロセスが有効なメッセージでは、3種類の検証を行なう。まず、ステップ8105で、ユーザIDを照合し、さらに検証し、ステップ8106で、ユーザIDを照合し、さらに、ステップ8107で、受信した情報の発行時刻を検証する。ステップ8107の発行時刻の検証では、受信した情報の発行時刻と、現在の時刻とのズレを検証し、ズレが時間TU(TU>0)以上である場合に、無効な情報であると判定する。したがって、ユーザのデジタル署名の検証にパスし、ユーザIDが一一致し、発行時刻の検証にパスした場合のみ、ユーザプロセスが有効なメッセージにパスしたと判定し、それ以外の場合は、フェイルしたと判定する。

〔1125〕また、図113(a)と、図114(a)は、それぞれ、クレジット決済端末とサービス提供システムとのリモートアクセス処理における、クレジット決済端末のリモートアクセスプロセスと、サービス・提供システムとの処理フローを示している。

〔1126〕リモートアクセス処理は、サービス・提供システム・ユーザプロセスに存在するデータにアクセスする、ことによって開始される。クレジット決済端末は、まず、ステップ8200で、アクセスするデータのリモートアクセス要求5400を生成し、ステップ8201で、ターミナル・ステータスから、セッション確立状態が否かを判定し、セッション確立状態の場合には、ステップ8203で、生成したリモートアクセス要求をサービス・提供システムに送信し、セッション確立状態でない場合には、ステップ8202でセッション確立処理を行ない、サービス提供システムとのセッションを確立してから、ステップ8203へ進む。

〔1127〕リモートアクセス要求を送信したクレジット決済端末は、ステップ8204とステップ8211とで、リモートアクセスデータ5401の受信を待つ。ステップ8204では、リモートアクセスデータの受信の判定を行ない、ステップ8211では、タイムアウトの判定を行なう。

〔1128〕ステップ8211のタイムアウトの判定では、タイムアウト時間TRM(TRM>0)以上の間、リモートアクセスデータを受信しない場合、クレジット決済端末はタイムアウトして、ステップ8212で、サービス・提供システム・ユーザプロセスに、サービス・提供システム・ユーザプロセスを送信し、サービス・提供システムとのセッションと回線を切断し、LCDに、タイムアウト・エラーを表示する。

〔1129〕リモートアクセスデータを受信した場合、クレジット決済端末は、ステップ8205で、サービス・提供システム・ユーザプロセスの暗号を復号化し、ステップ8206で、サービス・提供システム・ユーザプロセスの有効性を検証する。ユーザプロセスの有効性を検証する。

〔1130〕サービス・提供システムが有効なメッセージにパスした場合には、クレジット決済端末は、ステップ8207で、リモートアクセスデータのデータ5509の部分RAMのテンポラリ領域に格納し、ステップ8208で、データのアドレス情報を、データに格納したローカルアドレスに更新し、ステップ8209で、RAMに格納したデータにアクセスする。そして、ステップ8210で、テンポラリ領域の空き容量から、データアップロード処理が必要か否かを判定し、テンポラリ領域の空き容量が、設定値AM(AM>0)以上ある場合には、そのまま、リモートアクセス処理を終了し、設定値AMより少ない場合には、データアップロードプロセスを生成し、データアップロード処理へ進む。

〔1131〕サービス・提供システムが有効なメッセージにフェイルした場合には、クレジット決済端末は、ステップ8213で、サービス・提供システム・ユーザプロセス・エラー処理を行ない、リモートアクセス処理を終了する。サービス・提供システム・ユーザプロセス・エラー処理では、クレジット決済端末は、サービス・提供システム・ユーザプロセスにサービス・提供システム・ユーザプロセスを送信し、サービス・提供システムとのセッションと回線を切断し、LCDに、セッション・エラーを表示する。

〔1132〕また、サービス・提供システムが有効なメッセージは、サービス・提供システム・ユーザプロセスから受信したメッセージの有効性を検証する処理であり、図113(b)に示すように、サービス・提供システムが有効なメッセージでは、3種類の検証を行なう。まず、ステップ8314で、サービス提供者のデジタル署名を検証し、ステップ8315

で、サービス提供者IDを照合し、さらに、ステップ8316で、受信したメッセージの発行時刻を検証する。ステップ8316の発行時刻の検証では、受信した情報の発行時刻と、現在の時刻とのズレを検証し、ズレが時間TM(TM>0)以上である場合に、無効な情報であると判定する。したがって、サービス提供者IDが一一致し、発行時刻の検証にパスし、サービス提供者IDが一一致し、発行時刻の検証にパスした場合のみ、サービス・提供システムが有効なメッセージにパスしたと判定し、それ以外の場合は、フェイルしたと判定する。

〔1133〕一方、サービス・提供システムでは、リモートアクセス処理は、リモートアクセス要求5400を受信することによって開始される。サービス・提供システムは、まず、ステップ8300で、サービス提供者のプライバシー・レベルを、受信したリモートアクセス要求の暗号を復号化し、ステップ8301で、サービス・提供システムが有効なメッセージを行ない、リモートアクセス要求の有効性を検証する。

〔1134〕サービス・提供システムが有効なメッセージにパスした場合には、サービス・提供システムは、ステップ8302で、リモートアクセスデータ5401を生成し、ステップ8303で、生成したリモートアクセスデータをクレジット決済端末に送信して、リモートアクセス処理を終了する。

〔1135〕サービス・提供システムが有効なメッセージにフェイルした場合には、サービス・提供システムは、受信したメッセージは有効ではないと判定し、ステップ8304で、サービス・提供システム・ユーザプロセス・エラー処理を行ない、リモートアクセス処理を終了する。サービス・提供システム・ユーザプロセス・エラー処理によって、サービス・提供システム・ユーザプロセスにサービス・提供システム・ユーザプロセスを送信し、サービス・提供システムとのセッションと回線を切断される。この際、サービス・提供システムは、無効なメッセージを受信したことを示すセッション・エラーメッセージを、管理システム407に送信する。

〔1136〕また、サービス・提供システムが有効なメッセージは、クレジット決済端末から受信した情報の有効性を検証する処理であり、図114(b)に示すように、サービス・提供システムが有効なメッセージでは、3種類の検証を行なう。まず、ステップ8305で、サービス・提供システム・ユーザプロセスの署名を検証し、ステップ8306で、サービス・提供システム・ユーザプロセスの署名を照合し、さらに、ステップ8307で、受信した情報の発行時刻を検証する。ステップ8307の発行時刻の検証では、受信した情報の発行時刻と、現在の時刻とのズレを検証し、ズレが時間TU(TU>0)以上である場合に、無効な情報であると判定する。したがって、サービス・提供システムが有効なメッセージにパスし、サービス・提供システムが有効なメッセージにパスした場合のみ、サービス・提供システムが有効なメッセージにパスしたと判定し、それ以外の場合は、フェイルしたと判定する。



(1137) 次に、データアップデータ処理における処理フローについて説明する。

(1138) 図115と、図116は、それぞれ、パーソナル・クレジット端末とユーザ提供システムとのデータアップデータ処理における、パーソナル・クレジット端末のデータアップデータプロセスと、ユーザ提供システムのエラープロセスとの処理フローを示している。

(1139) データアップデータ処理は、パーソナル・クレジット端末のクロックカウンタの値が、アップデータ時刻レシタに一致した場合、または、テンボリ領域の空き容量が、設定値Aよりも少なくなった場合に、パーソナル・クレジット端末が、データアップデータプロセスを生成することによって開始される。

(1140) パーソナル・クレジット端末は、まず、ステップ8400で、LCDに“データアップデータ中”を表示し、ステップ8401で、データアップデータ要求8103を生成し、ステップ8402で、タミナル・スライタスから、セリジョン独立状態が否かを判定し、セリジョン独立状態の場合は、ステップ8404で、生成したデータアップデータ要求をユーザプロセスに送信し、セリジョン独立状態でない場合には、ステップ8403でセリジョン独立状態を行ない、ユーザ提供システムとのセリジョンを確立してから、ステップ8404へ進む。

(1141) データアップデータ要求を送信したパーソナル・クレジット端末は、ステップ8405とステップ8416とで、データアップデータ応答8103の受信を待つ。ステップ8405では、データアップデータ応答の受信を待たない、ステップ8416では、タイムアウトの判定を行なう。

(1142) ステップ8416のタイムアウトの判定では、タイムアウト時間T RUND (T RUND > 0) 以上の間、データアップデータ応答を受信しない場合、パーソナル・クレジット端末はタイムアウトして、ステップ8417で、ユーザ・タイムアウト・エラー処理を行ない、データアップデータ処理を終了する。

(1143) データアップデータ応答を受信した場合、パーソナル・クレジット端末は、ステップ8406で、ユーザのライバート鍵で、データアップデータ応答の暗号を復号化し、ステップ8407で、ユーザ有効性チェックを行ない、データアップデータ応答の有効性を検証する。

(1144) ユーザ有効性チェックにパスした場合には、パーソナル・クレジット端末は、ステップ8408で、RAMのデータをデータ圧縮して、アップロードデータ5104を生成し、ステップ8409で、生成したアップロードデータをユーザプロセスに送信する。

(1145) ユーザ有効性チェックにフェイルした場合

には、パーソナル・クレジット端末は、ステップ8418

で、ユーザ・セリジョン・エラー処理を行ない、データアップデータ処理を終了する。

(1146) アップロードデータを送信したパーソナル・クレジット端末は、ステップ8410とステップ8419とで、ユーザプロセスからのメッセージの受信を待つ。ステップ8410では、メッセージの受信を行ない、ステップ8419では、タイムアウトの判定を行なう。

(1147) ステップ8419のタイムアウトの判定では、タイムアウト時間T DU (T DU > 0) 以上の間、メッセージを受信しない場合、パーソナル・クレジット端末はタイムアウトして、ステップ8420で、ユーザ・タイムアウト・エラー処理を行ない、データアップデータ処理を終了する。

(1148) ユーザプロセスからのメッセージを受信した場合、パーソナル・クレジット端末は、ステップ8411で、ユーザのライバート鍵で、受信したメッセージの暗号を復号化し、ステップ8412で、ユーザ有効性チェックを行ない、受信したメッセージの有効性を検証する。

(1149) ユーザ有効性チェックにパスした場合には、パーソナル・クレジット端末は、ステップ8413へ進み、ユーザ有効性チェックにフェイルした場合には、パーソナル・クレジット端末は、ステップ8421で、ユーザ・セリジョン・エラー処理を行ない、データアップデータ処理を終了する。

(1150) パーソナル・クレジット端末は、ステップ8413では、受信したメッセージが、アップデータデータ5105か、機能停止命令5105かを判定し、アップデータデータであった場合には、ステップ8414で、アップデータデータの端末データ5133のデータ圧縮を解除して、RAMのデータを更新し、ステップ8415で、“データアップデータ中”の表示を解除して、データアップデータ処理を終了する。

(1151) 受信したメッセージが、機能停止命令であった場合には、パーソナル・クレジット端末は、ステップ8417で、LCDに“使用不能”を表示し、ステップ8418で、EEPROM5133の端末イネーブルのビットをクリアして、操作が出来ないようにし、ステップ8419で、タミナル・スライタスを使用不能に変更して、データアップデータ処理を終了する。

(1152) 一方、ユーザプロセスでは、データアップデータ処理は、データアップデータ要求8102を受信することによって開始される。ユーザプロセスは、まず、ステップ8500で、ユーザ提供者のライバート鍵で、受信したデータアップデータ要求の暗号を復号化し、ステップ8501で、ユーザプロセス有効性チェックを行ない、データアップデータ要求の有効性を検証する。

(1153) ユーザプロセス有効性チェックにパスした場合は、ユーザプロセスは、ステップ8502で、データアップデータ応答8103を生成し、ステップ8503で、生成したデータアップデータ応答をパーソナル・クレジット端末に送信する。

(1154) ユーザプロセス有効性チェックにフェイル

した場合には、ユーザプロセスは、受信したメッセージ

は有効ではないと判定し、ステップ8517で、ユーザプロ

セス・セリジョン・エラー処理を行ない、データアップ

データ処理を終了する。

(1155) データアップデータ応答を送信したユーザプロセスは、ステップ8504とステップ8515とで、アップロードデータ8104の受信を待つ。ステップ8504では、アップロードデータの受信を行ない、ステップ8515では、タイムアウトの判定を行なう。

(1156) ステップ8515のタイムアウトの判定では、タイムアウト時間T DU (T DU > 0) 以上の間、アップロードデータを受信しない場合、ユーザプロセスはタイムアウトして、ステップ8516で、ユーザプロセス・タイムアウト・エラー処理を行ない、データアップデータ処理を終了する。ユーザプロセスは、ユーザ・エラー処理によって、ユーザプロセスは、ユーザ・エラー・マネージメントによって消去され、パーソナル・クレジット端末とのセリジョンと同期は切断される。この際、ユーザプロセスは、タイムアウトしたことを示すタイムアウト・エラーメッセージを、管理システム407に送信する。

(1157) アップロードデータを受信した場合、ユーザプロセスは、ステップ8505で、ユーザ提供者のライバート鍵で、アップロードデータデータの暗号を復号化し、ステップ8506で、ユーザプロセス有効性チェックを行ない、アップロードデータの有効性を検証する。

(1158) ユーザプロセス有効性チェックにパスした場合は、ユーザプロセスは、ステップ8506へ進み、ユーザプロセス有効性チェックにフェイルした場合には、ユーザプロセスは、受信したメッセージは有効ではないと判定し、ステップ8517で、ユーザプロセス・セリジョン・エラー処理を行ない、データアップデータ処理を終了する。

(1159) ユーザプロセスは、ステップ8507で、アップロードデータの端末データ5131のデータ圧縮を解除し、ステップ8508で、データ圧縮を解除した端末データが、不正に改ざんされていないかを検証する。端末データと、ユーザ情報サバーの端末データ4105、及び、その他のユーザデータ管理情報4100によって管理されるデータとを照合する。

(1160) データ照合チェックにパスした場合には、ユーザプロセスは、まず、ステップ8509で、データ圧縮を解除した端末データを基に、ユーザ情報サバーのクレジットカード・リスと41008のアクセス時刻を、最新の情報に更新し、次に、ステップ8510で、パーソナル・クレジット端末の本体データ領域の容量と、データの生成時刻とアクセス時刻とに基づいて、新しい端末データを生成し、ステップ8511で、データ圧縮を解除した端末データと、新しい端末データとの差分をとって、アップデー

トデータ5105を生成して、ステップ8517で、生成したアップデータデータを、パーソナル・クレジット端末に送信し、8513で、ユーザ情報サバーの端末データ41006を更新して、データアップデータ処理を終了する。

(1161) データ照合チェックにフェイルした場合には、端末データが不正に改ざんされている可能性があるかと判断して、ユーザプロセスは、ステップ8518で、機能停止命令5105を生成し、ステップ8519で、生成した機能停止命令を、パーソナル・クレジット端末に送信し、さらに、ステップ8520で、ユーザ情報サバーのエラー・スライタス41012を“使用不能”に変更し、ステップ8521で、ユーザプロセス・セリジョン・エラー処理を行なう。

(1162) ステップ8520の新しい端末データの生成では、テンボリ領域が空になるように、RAMに格納するデータを再編成する。特に、本体データ領域21813の容量に余裕が無い場合には、各クレジットカードのアクセス時刻を比較して、アクセス時刻が最近のクレジットカードのオプジェクト・データ・アドレスにローカルアドレスを割り当て、また、各利用情報の利用時刻を比較して、利用時刻が最近の利用情報の利用情報アドレスにローカルアドレスを割り当てる。また、パーソナル・クレジット端末のプログラム・セリジョンアップする必要がある場合には、基本プログラム領域のデータを更新する。但し、ユーザ情報は、パーソナル・クレジット端末から受信した端末データのユーザ領域のデータに、更新される。

(1163) また、図117と、図118は、それぞれ、クレジット決済端末とユーザ提供システムとのデータアップデータ処理における、クレジット決済端末のデータアップデータプロセスと、ユーザ提供システムとのデータアップデータプロセスとを示している。

(1164) データアップデータ処理は、クレジット決済端末のクロックカウンタの値が、アップデータ時刻レシタに一致した場合、または、テンボリ領域の空き容量が、設定値Aよりも少なくなった場合に、クレジット決済端末が、データアップデータプロセスを生成することによって開始される。

(1165) クレジット決済端末は、まず、ステップ8600で、LCDに“データアップデータ中”を表示し、ステップ8601で、データアップデータ要求8402を生成し、ステップ8602で、タミナル・スライタスから、セリジョン独立状態が否かを判定し、セリジョン独立状態の場合は、ユーザ・タイムアウト・エラー処理を行ない、ユーザ・タイムアウト・エラー処理を行ない、データアップデータ要求を送信したクレジット決済端末は、ステップ8605とステップ8616とで、デ

ータアップデータ応答5403の受信を待つ。ステップ8605では、データアップデータ応答の受信の判定を行ない、ステップ8616では、タイムアウトの判定を行なう。

[1167] ステップ8616のタイムアウトの判定では、タイムアウト時間TUDM (TUDM > 0) 以上の間、データアップデータ応答を受信しない場合、クレジット決済端末はタイムアウトし、ステップ8617で、マーチャント・タイムアウト・エラー処理を行ない、データアップデータ処理を終了する。

[1168] データアップデータ応答を受信した場合、クレジット決済端末は、ステップ8606で、マーチャントのプライベートで、データアップデータ応答の暗号を復号化し、ステップ8607で、マーチャント有効性チェックを行ない、データアップデータ応答の有効性を検証する。

[1169] マーチャント有効性チェックにパスした場合には、クレジット決済端末は、ステップ8608で、RAM、及び、ハードディスクのデータ・データ圧縮して、アップロードデータを送信し、ステップ8609で、生成したアップロードデータをマーチャントプロセッサに送信する。

[1170] マーチャント有効性チェックにフェイルした場合には、クレジット決済端末は、ステップ8618で、マーチャント・セッション・エラー処理を行ない、データアップデータ処理を終了する。

[1171] アップロードデータを送信したクレジット決済端末は、ステップ8610とステップ8619とで、マーチャントプロセッサからのメッセージの受信を待つ。ステップ8610では、メッセージの受信の判定を行ない、ステップ8619では、タイムアウトの判定を行なう。

[1172] ステップ8619のタイムアウトの判定では、タイムアウト時間TDM (TDM > 0) 以上の間、メッセージを受信しない場合、クレジット決済端末はタイムアウトして、ステップ8620で、マーチャント・タイムアウト・エラー処理を行ない、データアップデータ処理を終了する。

[1173] マーチャントプロセッサからのメッセージを受信した場合、クレジット決済端末は、ステップ8611で、マーチャントのプライベートで、受信したメッセージの暗号を復号化し、ステップ8612で、マーチャント有効性チェックを行ない、受信したメッセージの有効性を検証する。

[1174] マーチャント有効性チェックにパスした場合には、クレジット決済端末は、ステップ8613へ進む。マーチャント有効性チェックにフェイルした場合には、マーチャント有効性チェックにフェイルした場合には、クレジット決済端末は、ステップ8621で、マーチャント・セッション・エラー処理を行ない、データアップデータ処理を終了する。

[1175] クレジット決済端末は、ステップ8613では、受信したメッセージが、アップデータデータ5405

か、機能停止命令5405かを判定し、アップデータデータであった場合には、ステップ8614で、アップデータデータの端末データ5539のデータ圧縮を解除して、RAM、及び、ハードディスクのデータを更新し、ステップ8615で、"データアップデータ中"の表示を解除して、データアップデータ処理を終了する。

[1176] 受信したメッセージが、機能停止命令であった場合には、クレジット決済端末は、ステップ8622で、LCDに"使用不能"を表示し、ステップ8623で、EEPROM2504の端末キーのビットをクリアして、操作が出来ないようにし、ステップ8624で、ターミナル・ステイタスを使用不能に変更して、データアップデータ処理を終了する。

[1177] 一方、マーチャントプロセッサでは、データアップデータ処理は、データアップデータ要求5402を受信することによって開始される。マーチャントプロセッサは、まず、ステップ8700で、サービス提供者のプライベートで、受信したデータアップデータ要求の暗号を復号化し、ステップ8701で、マーチャントプロセッサ有効性チェックを行ない、データアップデータ要求の有効性を検証する。

[1178] マーチャントプロセッサ有効性チェックにパスした場合には、マーチャントプロセッサは、ステップ8702で、データアップデータ応答5403を生成し、ステップ8703で、生成したデータアップデータ応答をクレジット決済端末に送信する。

[1179] マーチャントプロセッサ有効性チェックにフェイルした場合には、マーチャントプロセッサは、受信したメッセージは有効ではないと判定し、ステップ8713で、マーチャントプロセッサ・セッション・エラー処理を行ない、データアップデータ処理を終了する。

[1180] データアップデータ応答を送信したマーチャントプロセッサは、ステップ8704とステップ8714とで、アップロードデータ5404の受信を待つ。ステップ8704では、アップロードデータの受信の判定を行ない、ステップ8714では、タイムアウトの判定を行なう。

[1181] ステップ8714のタイムアウトの判定では、タイムアウト時間TUDM (TUDM > 0) 以上の間、アップロードデータを受信しない場合、マーチャントプロセッサはタイムアウトして、ステップ8715で、マーチャントプロセッサ・タイムアウト・エラー処理を行ない、データアップデータ処理を終了する。マーチャントプロセッサ・タイムアウト・エラー処理によって、マーチャントプロセッサは、サービス・マネージャプロセッサによって消去され、クレジット決済端末とのセッションと回線は切断される。この際、マーチャントプロセッサは、タイムアウトしたことを示すタイムアウト・エラーメッセージを、管理システム401に送信する。

[1182] アップロードデータを受信した場合、マーチャントプロセッサは、ステップ8705で、サービス提供者

のプライベートで、受信したアップロードデータの暗号を復号化し、ステップ8706で、マーチャントプロセッサ有効性チェックを行ない、アップロードデータの有効性を検証する。

[1183] マーチャントプロセッサ有効性チェックにパスした場合には、マーチャントプロセッサは、ステップ8707へ進む。マーチャントプロセッサ有効性チェックにフェイルした場合には、マーチャントプロセッサは、受信したメッセージは有効ではないと判定し、ステップ8716で、マーチャントプロセッサ・セッション・エラー処理を行ない、データアップデータ処理を終了する。

[1184] マーチャントプロセッサは、ステップ8707で、アップロードデータの端末データ5531のデータ圧縮を解除し、ステップ8708で、データ照合チェックを行ない、端末データが、不正に改ざんされていないかを検証する。データ照合チェックでは、データ圧縮を解除した端末データと、マーチャント情報サーバの端末データ24006、及び、その他のマーチャントデータ管理情報24000によって管理されるデータとを照合する。

[1185] データ照合チェックにパスした場合には、マーチャントプロセッサは、まず、ステップ8709で、クレジット決済端末の端末データ領域の容量と、データの生成時刻に基づいて、新しい端末データを生成し、ステップ8710で、データ圧縮を解除した端末データと、新しい端末データとの差分をとり、アップデータデータ5405を生成して、ステップ8711で、生成したアップデータデータを、クレジット決済端末に送信し、8712で、マーチャント情報サーバの端末データ24104を更新して、データアップデータ処理を終了する。

[1186] データ照合チェックをフェイルした場合には、端末データが不正に改ざんされている可能性がある。と判断して、マーチャントプロセッサは、ステップ8717で、機能停止命令5405を生成し、ステップ8718で、生成した機能停止命令を、クレジット決済端末に送信し、さらに、ステップ8719で、マーチャント情報サーバ上のマーチャント・ステイタス24015を"使用不能"に変更し、ステップ8720で、マーチャントプロセッサ・セッション・エラー処理を行なって、データアップデータ処理を終了する。

[1187] ステップ8709の新しい端末データの生成では、テンポラリ領域が空になるように、RAM、及び、ハードディスクに格納するデータを再構成する。特に、実データ領域の容量に余裕が無い場合には、各販売情報領域の時刻を比較して、販売時刻が最近の販売情報にロケアルアドレスを割り当て、クレジット決済端末のプログラムをバージョンアップする必要がある場合には、基本プログラム領域のデータも更新する。但し、マーチャント領域は、クレジット決済端末から受信した端末データのマーチャント領域のデータに、更新される。

[1188] 次に、強制的データアップデータ処理にお

ける処理フローについて説明する。図119と、図120は、それぞれ、パーソナル・クレジット端末とサービス提供システムとの強制的データアップデータ処理における、パーソナル・クレジット端末の強制的データアップデータプロセッサと、サービス提供システムのユーザプロセッサとの処理フローを示している。

[1189] 強制的データアップデータ処理は、サービス提供システム102が、ユーザとの契約内容に変更があった場合など、パーソナル・クレジット端末100のRAMのデータを、再更新する必要がある場合に行なう。

[1190] ユーザプロセッサは、まず、ステップ8900で、データアップデータ命令5106を生成し、ステップ8901で、ターミナル・ステイタスから、セッション確立状態かを判定し、セッション確立状態の場合には、セッション8903で、生成したデータアップデータ命令をパーソナル・クレジット端末に送信し、セッション確立状態でない場合には、ステップ8902でセッション確立処理を行ない、サービス提供システムとのセッションを確立してから、ステップ8903へ進む。

[1191] データアップデータ命令を送信したユーザプロセッサは、ステップ8904とステップ8914とで、アップロードデータ5107の受信を待つ。ステップ8904では、アップロードデータの受信の判定を行ない、ステップ8914では、タイムアウトの判定を行なう。

[1192] ステップ8914のタイムアウトの判定では、タイムアウト時間TUDU (TUDU > 0) 以上の間、アップロードデータを受信しない場合、ユーザプロセッサはタイムアウトして、ステップ8915で、ユーザプロセッサ・タイムアウト・エラー処理を行ない、強制的データアップデータ処理を終了する。

[1193] アップロードデータを受信した場合、ユーザプロセッサは、ステップ8905で、サービス提供者のプライベートで、受信したアップロードデータの暗号を復号化し、ステップ8906で、ユーザプロセッサ有効性チェックを行ない、アップロードデータの有効性を検証する。[1194] ユーザプロセッサ有効性チェックにパスした場合には、ユーザプロセッサは、ステップ8907へ進む。ユーザプロセッサ有効性チェックにフェイルした場合には、ユーザプロセッサは、受信したメッセージは有効ではないと判定し、ステップ8916で、ユーザプロセッサ・セッション・エラー処理を行ない、強制的データアップデータ処理を終了する。

[1195] ユーザプロセッサは、ステップ8907で、アップロードデータの端末データ5331のデータ圧縮を解除し、ステップ8908で、データ照合チェックを行ない、端末データが、不正に改ざんされていないかを検証する。[1196] データ照合チェックにパスした場合には、ユーザプロセッサは、まず、ステップ8909で、データ圧縮を解除した端末データを基に、ユーザ情報サーバのクレ、

(109)

ソフトカー・リミット34006のアクセス時刻を、最新の時刻に変更し、次に、スレッツ78910で、パーソナル・クレジット端末の本体データ領域の容量と、データの生成時刻とアクセス時刻に基づいて、新しい端末データを生成し、スレッツ8811で、データ圧縮を解除した端末データと、新しい端末データとの差分をとって、フロッピーデータ5106を生成して、スレッツ78913で、生成したフロッピーデータを、パーソナル・クレジット端末に送信し、スレッツ78913で、ユーザ情報サバの端末データ24006を更新して、強制的データアップグレード処理を終了する。

(1197) データ照合チェックをフェイルした場合には、端末データが不正に改ざんされている可能性があるとして判断して、ユーザプロセスは、スレッツ8917で、機能停止命令5108を生成し、スレッツ78916で、生成した機能停止命令を、パーソナル・クレジット端末に送信し、さらに、スレッツ78919で、ユーザ情報サバ上のユーザ・ステータス34012を“使用不能”に変更し、スレッツ78920で、ユーザプロセス・セッションエラー処理を行なう。強制的データアップグレード処理を終了する。

(1198) スレッツ78910の新しい端末データの生成では、テンポラリ領域が空になるように、RAMに格納するデータを再編成する。特に、本体データ領域21812の容量に余裕が無い場合には、各クレジットカーのアクセス時刻を比較して、アクセス時刻が最近のクレジットカーのアクセス・データ・アドレスにローカルアドレスを割り当て、また、各利用情報の利用情報アドレスに、利用時刻が最近の利用情報アドレスにローカルアドレスを割り当てる。また、パーソナル・クレジット端末のプログラムをバージョンアップする必要のある場合には、基本プログラム領域のデータを更新する。但し、ユーザ領域は、パーソナル・クレジット端末から受信した端末データのユーザ領域のデータに、更新される。

(1199) 一方、パーソナル・クレジット端末では、強制的データアップグレード処理は、データアップグレード命令5106を受信して、強制的データアップグレードプロセスを生成することによって開始される。

(1200) パーソナル・クレジット端末は、まず、スレッツ78907で、ユーザのライベリで、データアップグレード命令の暗号を復号化し、スレッツ78901で、ユーザ有効性チェックを行ない、データアップグレード命令の有効性を検証する。

(1201) ユーザ有効性チェックにパスした場合には、パーソナル・クレジット端末は、スレッツ78902で、LCDに“データアップグレード中”を表示し、スレッツ78903で、RAMのデータをデータ圧縮して、フロッピーデータ5107を生成し、スレッツ78904で、生成したフロッピーデータをユーザプロセスに送信する。

(1202) ユーザ有効性チェックにフェイルした場合

には、パーソナル・クレジット端末は、スレッツ78911で、ユーザ・セッション・エラー処理を行ない、強制的データアップグレード処理を終了する。

(1203) フロッピーデータを送信したパーソナル・クレジット端末は、スレッツ78905とスレッツ78912とで、ユーザプロセスからのメッセージの受信を待つ。スレッツ78905では、メッセージの受信の判定を行ない、スレッツ78912では、タイムアウトの判定を行なう。

(1204) スレッツ78913のタイムアウトの判定では、タイムアウト時間(TMO (TMO > 0) 以上の間、メッセージを受信しない場合、パーソナル・クレジット端末はタイムアウトして、スレッツ78913で、ユーザ・タイムアウト・エラー処理を行ない、強制的データアップグレード処理を終了する。

(1205) ユーザプロセスからのメッセージを受信した場合、パーソナル・クレジット端末は、スレッツ78906で、ユーザのライベリで、受信したメッセージの暗号を復号化し、スレッツ78907で、ユーザ有効性チェックを行ない、受信したメッセージの有効性を検証する。

(1206) ユーザ有効性チェックにパスした場合には、パーソナル・クレジット端末は、スレッツ78908へ進み、ユーザ有効性チェックにフェイルした場合には、パーソナル・クレジット端末は、スレッツ78914で、ユーザ・セッション・エラー処理を行ない、強制的データアップグレード処理を終了する。

(1207) パーソナル・クレジット端末は、スレッツ78908で、受信したメッセージがフロッピーデータ5106が、機能停止命令5106を判定し、アップグレードデータであった場合には、スレッツ78909で、フロッピーデータの端末データ5533のデータ圧縮を解除して、RAMのデータを更新し、スレッツ78910で、“データアップグレード中”の表示を解除して、強制的データアップグレード処理を終了する。

(1208) 受信したメッセージが、機能停止命令であった場合には、パーソナル・クレジット端末は、スレッツ78915で、LCDに“使用不能”を表示し、スレッツ78916で、EEPROM5103の端末キーネーブルのビットをクリアして、操作が出来ないようにし、スレッツ78917で、ターミナル・ステータスを使用不能に変更して、強制的データアップグレード処理を終了する。

(1209) また、図121と、図122は、それぞれ、クレジット技術端末とサビエ提供システムとの強制的データアップグレード処理における、クレジット技術端末の強制的データアップグレードプロセスと、サビエ提供システムのデータアップグレードの処理フローを示している。

(1210) 強制的データアップグレード処理は、サビエ提供システム4107が、データアップグレードの実行内容に変更があった場合など、クレジット技術端末101のRAM、及び、ハードウェアのデータを、早急に更新する

(110)

必要がある場合に行なう。

(1211) データアップグレードプロセスは、まず、スレッツ9100で、データアップグレード命令5106を生成し、スレッツ79101で、ターミナル・ステータスから、セッション確立情報か否かを判定し、セッション確立状態の場合には、スレッツ79103で、生成したデータアップグレード命令をクレジット技術端末に送信し、セッション確立状態でない場合には、スレッツ9102でセッション確立処理を行ない、サビエ提供システムとのセッションを確立してから、スレッツ79103へ進む。

(1212) データアップグレード命令を送信したデータアップグレードプロセスは、スレッツ9104とスレッツ9113とで、フロッピーデータ5407の受信を待つ。スレッツ9104では、フロッピーデータの受信の判定を行ない、スレッツ79113では、タイムアウトの判定を行なう。

(1213) スレッツ9113のタイムアウトの判定では、タイムアウト時間(TMO (TMO > 0) 以上の間、フロッピーデータを受信しない場合、データアップグレードプロセスをフェイルしたとして、スレッツ9114で、データアップグレード・タイムアウト・エラー処理を行ない、強制的データアップグレード処理を終了する。

(1214) フロッピーデータを受信した場合、データアップグレードプロセスは、スレッツ9105で、サビエ提供者のライベリで、受信したフロッピーデータの暗号を復号化し、スレッツ9106で、データアップグレードの有効性チェックを行ない、フロッピーデータの有効性を検証する。

(1215) データアップグレードプロセスがフェイルした場合には、データアップグレードプロセスは、スレッツ9107へ進み、データアップグレード有効性チェックにフェイルした場合には、データアップグレードプロセスは、受信したメッセージは有効ではないと判定し、スレッツ9115で、データアップグレード・セッション・エラー処理を行ない、強制的データアップグレード処理を終了する。

(1216) データアップグレードプロセスは、スレッツ9107で、フロッピーデータの端末データ5533のデータ圧縮を解除し、スレッツ9108で、データ照合チェックを行ない、端末データが、不正に改ざんされていないかを検証する。

(1217) データ照合チェックにパスした場合には、データアップグレードプロセスは、スレッツ9109で、クレジット技術端末の本体データ領域の容量と、データの生成時刻に基づいて、新しい端末データを生成し、スレッツ79110で、データ圧縮を解除した端末データと、新しい端末データとの差分をとって、フロッピーデータ5408を生成して、スレッツ9111で、生成したフロッピーデータを、クレジット技術端末に送信し、スレッツ9112で、データアップグレード・セッション・エラー処理を行なう。強制的データアップグレード処理を終了する。

(1218) データ照合チェックにフェイルした場合

には、端末データが不正に改ざんされている可能性があるとして判断して、データアップグレードプロセスは、スレッツ9116で、機能停止命令5408を生成し、スレッツ79117で、生成した機能停止命令を、クレジット技術端末に送信し、さらに、スレッツ9118で、データアップグレード・セッション・エラー・ステータス34012を“使用不能”に変更し、スレッツ9119で、データアップグレード・セッション・エラー処理を行なう。強制的データアップグレード処理を終了する。

(1219) スレッツ9109の新しい端末データの生成では、テンポラリ領域が空になるように、RAM、及び、ハードウェアに格納するデータを再編成する。特に、本体データ領域の容量に余裕が無い場合には、各販売情報の販売時刻を比較して、販売時刻が最近の販売情報にローカルアドレスを割り当て、また、各利用情報のプログラムをバージョンアップする必要のある場合には、基本プログラム領域のデータを更新する。但し、データアップグレード領域は、クレジット技術端末から受信した端末データアップグレード命令の暗号を復号化し、スレッツ9001で、データアップグレード有効性チェックを行ない、データアップグレード命令の有効性を検証する。

(1220) データアップグレード有効性チェックにパスした場合には、クレジット技術端末は、スレッツ9002で、LCDに“データアップグレード中”を表示し、スレッツ9003で、RAM、及び、ハードウェアのデータをデータ圧縮して、フロッピーデータ5407を生成し、スレッツ9004で、生成したフロッピーデータをデータアップグレードプロセスに送信する。

(1221) データアップグレード有効性チェックにフェイルした場合には、クレジット技術端末は、スレッツ9004で、LCDに“データアップグレード中”を表示し、スレッツ9003で、RAM、及び、ハードウェアのデータをデータ圧縮して、フロッピーデータ5407を生成し、スレッツ9004で、生成したフロッピーデータをデータアップグレードプロセスに送信する。

(1222) データアップグレード有効性チェックにパスした場合には、クレジット技術端末は、スレッツ9004で、LCDに“データアップグレード中”を表示し、スレッツ9003で、RAM、及び、ハードウェアのデータをデータ圧縮して、フロッピーデータ5407を生成し、スレッツ9004で、生成したフロッピーデータをデータアップグレードプロセスに送信する。

(1223) データアップグレード有効性チェックにフェイルした場合には、クレジット技術端末は、スレッツ9001で、データアップグレード・セッション・エラー処理を行ない、強制的データアップグレード処理を終了する。

(1224) フロッピーデータを送信したクレジット技術端末は、スレッツ9005とスレッツ79012とで、データアップグレードプロセスからのメッセージの受信を待つ。スレッツ79005では、メッセージの受信の判定を行ない、スレッツ79012では、タイムアウトの判定を行なう。

(1225) スレッツ79012のタイムアウトの判定では、タイムアウト時間(TMO > 0) 以上の間、メッセージを受信しない場合、クレジット技術端末はタイムアウトして、スレッツ79013で、データアップグレード・タイムアウト・エラー処理を行ない、強制的データアップグレード処理を終了する。

【1226】マーチャントプロセスからのメッセージを受信した場合、クレジット決済端末は、ステップ9006で、マーチャントのプライベートルールで、受信したメッセージの暗号を復号化し、ステップ9007で、マーチャントの有効性チェックを行ない、受信したメッセージの有効性を検証する。

【1227】マーチャント有効性チェックにパスした場合には、クレジット決済端末は、ステップ9008へ進み、マーチャント有効性チェックにフェイルした場合には、クレジット決済端末は、ステップ9004で、マーチャント・セッション・エラー処理を行ない、強制のデータアップデート処理を終了する。

【1228】クレジット決済端末は、ステップ9008では、受信したメッセージが、アップデートデータ408か、機能停止命令5408かを判定し、アップデートデータであった場合には、ステップ9009で、アップデートデータの端末データ5539のデータ圧縮を解除して、RAM、及び、ハードディスクのデータを更新し、ステップ9010で、“データアップデート中”の表示を解除して、強制のデータアップデート処理を終了する。

【1229】受信したメッセージが、機能停止命令であった場合には、クレジット決済端末は、ステップ9015で、LCDに“使用不能”を表示し、ステップ9016で、EEPROM503の端末マイネームのビットをクリアし、操作が出来ないようにし、ステップ9017で、ターミナル・ステータスを使用不能に変更して、強制のデータアップデート処理を終了する。

【1230】次に、データバックアップ処理における処理フローについて説明する。

【1231】図123と、図116は、それぞれ、パーソナル・クレジット決済端末とサービス提供システムとのデータバックアップ処理における、パーソナル・クレジット決済端末のデータアップデートプロセスと、サービス提供システムのユーザプロセスとの処理フローを示しており、ユーザプロセスの処理は、データアップデート処理と同じである。

【1232】データバックアップ処理は、パーソナル・クレジット決済端末のバッテリ容量がQ以下になった場合には、パーソナル・クレジット決済端末が、データバックアッププロセスを生成することによって開始される。

【1233】パーソナル・クレジット決済端末は、まず、ステップ9300で、LCDに“データアップデート中”を表示し、ステップ9301で、データアップデート要求5109を生成し、ステップ9302で、ターミナル・ステータスから、セッション確立状態が否かを判定し、セッション確立状態の場合には、ステップ9304で、生成したデータアップデート要求をユーザプロセスに送信し、セッション確立状態でない場合には、ステップ9303でセッション確立処理を行ない、サービス提供システムとのセッションを確立してから、ステップ9304へ進む。

【1234】データアップデート要求を送信したパーソナル・クレジット決済端末は、ステップ9305とステップ9316とで、データアップデート要求5110の受信を待つ。ステップ9305では、データアップデート要求の受信の判定を行ない、ステップ9316では、タイムアウトの判定を行なう。

【1235】ステップ9316のタイムアウトの判定では、タイムアウト時間TTRM (TTRM > 0) 以上の間、データアップデート要求を受信しない場合、パーソナル・クレジット決済端末はタイムアウトして、ステップ9317で、ユーザ・タイムアウト・エラー処理を行ない、データバックアップ処理を終了する。

【1236】データアップデート要求を受信した場合、パーソナル・クレジット決済端末は、ステップ9306で、ユーザのプライベートルールで、データアップデート要求の暗号を復号化し、ステップ9307で、ユーザ有効性チェックを行ない、データアップデート要求の有効性を検証する。

【1237】ユーザ有効性チェックにパスした場合には、パーソナル・クレジット決済端末は、ステップ9308で、RAMのデータをデータ圧縮して、アップロードデータ5111を生成し、ステップ9309で、生成したアップロードデータをユーザプロセスに送信する。

【1238】ユーザ有効性チェックにフェイルした場合には、パーソナル・クレジット決済端末は、ステップ9318で、ユーザ・セッション・エラー処理を行ない、データバックアップ処理を終了する。

【1239】アップロードデータを送信したパーソナル・クレジット決済端末は、ステップ9310とステップ9319で、ユーザプロセスからのメッセージの受信を待つ。ステップ9310では、メッセージの受信の判定を行ない、ステップ9319では、タイムアウトの判定を行なう。

【1240】ステップ9319のタイムアウトの判定では、タイムアウト時間TTO (TTO > 0) 以上の間、メッセージを受信しない場合、パーソナル・クレジット決済端末はタイムアウトして、ステップ9320で、ユーザ・タイムアウト・エラー処理を行ない、データバックアップ処理を終了する。

【1241】ユーザプロセスからのメッセージを受信した場合、パーソナル・クレジット決済端末は、ステップ9321で、ユーザのプライベートルールで、受信したメッセージの暗号を復号化し、ステップ9322で、ユーザ有効性チェックを行ない、受信したメッセージの有効性を検証する。

【1242】ユーザ有効性チェックにパスした場合には、パーソナル・クレジット決済端末は、ステップ9318へ進み、ユーザ有効性チェックにフェイルした場合には、パーソナル・クレジット決済端末は、ステップ9321で、ユーザ・セッション・エラー処理を行ない、データバックアップ処理を終了する。

【1243】パーソナル・クレジット決済端末は、ステップ9313では、受信したメッセージが、アップデートデータ

5112か、機能停止命令5112かを判定し、アップデートデータであった場合には、まず、ステップ9314で、アップデートデータの端末データ539のデータ圧縮を解除し、RAMのデータを更新し、ステップ9315で、“ローバテリイ”表示をし、さらに、ステップ9325で、ターミナル・ステータスを、“ライト・プロテクティッド”に変更して、新たなデータがRAMに書き込まれないようにして、データバックアップ処理を終了する。

【1244】受信したメッセージが、機能停止命令であった場合には、パーソナル・クレジット決済端末は、ステップ9322で、LCDに“使用不能”を表示し、ステップ9323で、EEPROM503の端末マイネームのビットをクリアして、操作が出来ないようにし、ステップ9324で、ターミナル・ステータスを使用不能に変更して、データバックアップ処理を終了する。

【1245】次に、“決済”の処理における処理フローについて説明する。

【1246】図124から図125は、“決済”の処理におけるクレジット決済端末の処理フローを示している。“決済”の処理は、マーチャントが、レジスタのクレジット決済スイッチを押すと、クレジット決済端末300が、決済プロセスを生成することによって開始される。

【1247】クレジット決済端末は、まず、ステップ9300で、パーソナル・クレジット決済端末から受信する支払オフアーム5700の内容に対応する4種類の支払オフアーム5701を生成する。4種類の支払オフアーム5701は、ユーザが指定した支払金額が、マーチャントの請求金額よりも低いことを示す支払オフアーム5702と、マーチャントが取り扱えないクレジットカードを、ユーザが指定していることを示す支払オフアーム5703と、マーチャントが取り扱えない支払オフアーム5704と、ユーザが指定していることを示す支払オフアーム5705と、マーチャントが取り扱えないクレジットカードの取扱い不可を示す、ステップ9302へ戻り、再び、支払オフアームの受信を待つ。

【1248】この4種類の支払オフアーム5701は、それぞれ、支払オフアーム5702 (図89 (b) ) の支払メッセージ5809とクレジットカード番号5810との部分のみであり、ユーザが指定した支払金額がマーチャントの請求金額よりも低いことを示す支払オフアーム5702の場合には、支払オフアーム5702で、支払オフアーム5702と、マーチャントが取り扱えないクレジットカードを、ユーザが指定していることを示す支払オフアーム5703と、マーチャントが取り扱えない支払オフアーム5704と、ユーザが指定していることを示す支払オフアーム5705と、マーチャントが取り扱えないクレジットカードの取扱い不可を示す、ステップ9302へ戻り、再び、支払オフアームの受信を待つ。

され、トランザクション番号にはゼロが設定される。そして、ユーザの支払オフアームをマーチャントが取り扱えることを示す支払オフアーム5702の場合には、支払オフアーム5702に、グリーンディジットメッセージが設定され、トランザクション番号に、ユーザとの取引をユニークに示すゼロ以外の番号が設定される。

【1249】4種類の支払オフアーム5702を生成したクレジット決済端末は、ステップ9301で、LCDに“支払操作待ち”を表示して、ステップ9302で、支払オフアーム5700の受信を待つ。

【1250】パーソナル・クレジット決済端末から、支払オフアームを受信すると、クレジット決済端末は、ステップ9303からステップ9305で、受信した支払オフアームの内容を検証する。

【1251】支払オフアームの支払金額が、請求金額よりも小さい場合には、クレジット決済端末は、ステップ9317へ進み、ユーザが指定した支払金額が、マーチャントの請求金額よりも低いことを示す支払オフアーム5703を、パーソナル・クレジット決済端末へ送信し、パーソナル・クレジット決済端末の不足を表示して、ステップ9318で、LCDに支払金額の不足を表示して、ステップ9302へ戻り、再び、支払オフアームの受信を待つ。

【1252】また、支払オフアームのサービスコードが、クレジット決済端末のサービスコード・リストに存在しない場合には、クレジット決済端末は、ステップ9319へ進み、マーチャントが取り扱えないクレジットカードを進み、ユーザが指定していることを示す支払オフアーム5703を、パーソナル・クレジット決済端末へ送信し、パーソナル・クレジット決済端末の不足を表示して、ステップ9320で、LCDにクレジットカードの取扱い不可を示す、ステップ9302へ戻り、再び、支払オフアームの受信を待つ。

【1253】また、支払オフアームの支払オフアーム5702が、クレジット決済端末のサービスコード・リストに存在しない場合には、クレジット決済端末は、ステップ9321へ進み、マーチャントが取り扱えない支払オフアーム5703を、ユーザが指定していることを示す支払オフアーム5704を、パーソナル・クレジット決済端末へ送信し、パーソナル・クレジット決済端末の不足を表示して、ステップ9322で、LCDに支払オフアーム5704の取扱い不可を示す、ステップ9302へ戻り、再び、支払オフアームの受信を待つ。

【1254】それ以外の場合には、クレジット決済端末は、ステップ9306へ進み、ユーザの支払オフアームをマーチャントが取り扱えることを示す支払オフアーム5702を、パーソナル・クレジット決済端末へ送信し、パーソナル・クレジット決済端末は、ステップ9307で、支払オフアーム5702と、支払オフアーム5703と、マーチャントが取り扱えないクレジットカードを、ユーザが指定していることを示す支払オフアーム5704と、マーチャントが取り扱えない支払オフアーム5705と、マーチャントが取り扱えないクレジットカードの取扱い不可を示す、ステップ9302へ戻り、再び、支払オフアームの受信を待つ。

(113)

に送信し、セリジョン確立状態でない場合には、スレッ  
フ9310でセリジョン確立処理を行ない、サービス提供シ  
ステムとのセリジョンを確立してから、スレッフ9311へ  
進む。

〔1255〕 借用照会要求を送信したクレジット決済端  
末は、スレッフ9312とスレッフ9313とで、借用照会応答  
5700の受信待つ。スレッフ9312では、借用照会応答の  
受信の判定を行ない、スレッフ9313では、タイムアウ  
トの判定を行なう。

〔1256〕 スレッフ9313のタイムアウトの判定では、  
タイムアウト時間TAR (TAR > 0) 以上の間、借用照  
会応答を受信しない場合、クレジット決済端末はタイム  
アウトして、スレッフ9314で、ワーチャント・タイムア  
ウト・エラー処理を行ない、“決済”の処理を終了す  
る。

〔1257〕 借用照会応答を受信した場合、クレジット  
決済端末は、スレッフ9315で、ワーチャントのグライ  
ベート間で、借用照会応答の暗号を復号化し、スレッフ93  
14で、ワーチャント有効性チェックを行ない、借用照会  
応答の有効性を検証する。

〔1258〕 ワーチャント有効性チェックにパスした場  
合には、クレジット決済端末は、スレッフ9315へ進み、  
ワーチャント有効性チェックにフェイルした場合には、  
スレッフ9315で、ワーチャント・セリジョン・エラー処  
理を行ない、“決済”の処理を終了する。

〔1259〕 クレジット決済端末は、スレッフ9315で、  
借用照会応答の借用照会結果を判定し、借用照会をフ  
ェイルした場合には、スレッフ9316で、LCDに借用照会  
結果を表示して、“決済”の処理を終了し、借用照会を  
パスした場合には、スレッフ9316で、LCDに借用照会  
結果に、ユーザ個人データの内容を表示する。

〔1260〕 LCDに借用照会結果と、ユーザ個人デー  
タの内容を表示したクレジット決済端末は、スレッフ94  
00でスレッフ9411とで、ワーチャントによる決済処理要  
求操作5016を持つ。スレッフ9400では、ワーチャント  
による決済処理要求操作の判定を行ない、スレッフ9413  
では、タイムアウトの判定を行なう。

〔1261〕 スレッフ9413のタイムアウトの判定では、  
タイムアウト時間TMO (TMO > 0) 以上の間、ワー  
チャントによる決済処理要求操作が行なわれない場合、ク  
レジット決済端末はタイムアウトして、スレッフ9414  
で、ワーチャント・タイムアウト・エラー処理を行な  
い、“決済”の処理を終了する。

〔1262〕 ワーチャントによる決済処理要求操作が行  
なわれた場合、クレジット決済端末は、スレッフ9401  
で、LCDに“決済実行中”を表示し、スレッフ9402  
で、支払オフラーと支払オフラー応答とから、決済要求  
5705を生成し、スレッフ9405で、生成した決済要求5705  
をワーチャントプロセスに送信する。

〔1263〕 決済要求5705をワーチャントプロセスに送

信したクレジット決済端末は、スレッフ9404とスレッフ  
9415とで、ワーチャントプロセスから、決済完了通知57  
08を受信するの待つ。スレッフ9404では、決済完了通  
知5708の受信の判定を行ない、スレッフ9415では、タ  
イムアウトの判定を行なう。

〔1264〕 スレッフ9415のタイムアウトの判定では、  
タイムアウト時間TSPC (TSPC > 0) 以上の間、決済  
完了通知5708を受信しない場合、クレジット決済端末  
はタイムアウトして、スレッフ9416で、ワーチャント・  
タイムアウト・エラー処理を行ない、“決済”の処理を  
終了する。

〔1265〕 決済完了通知5708を受信した場合、クレ  
ジット決済端末は、スレッフ9405で、ワーチャントのグ  
ライベート間で、受信した決済完了通知5708の暗号を復号  
化し、スレッフ9406で、ワーチャント有効性チェックを  
行ない、受信したメッセージの有効性を検証する。

〔1266〕 ワーチャント有効性チェックにパスした場  
合には、クレジット決済端末は、スレッフ9407へ進み、  
ワーチャント有効性チェックにフェイルした場合には、  
クレジット決済端末は、スレッフ9417で、ワーチャント  
・セリジョン・エラー処理を行ない、“決済”の処理を  
終了する。

〔1267〕 クレジット決済端末は、スレッフ9407で、  
領収書5709を生成し、スレッフ9408で、生成した領収書  
5709を、ワーチャントプロセスへ送信する。そして、ス  
レッフ9409で、暗号を復号化した決済完了通知5708をR  
AMのデータリ領域に格納し、スレッフ9410で、販売  
履歴リストと、販売履歴リスト・アドレスとを更新し  
て、スレッフ9411で、LCDに、“決済完了”を表示す  
る。そして、スレッフ9412で、データリ領域の空き容  
量から、データリ領域の空き容量が、設定値AM (AM >  
0) 以上ある場合には、そのまま、“決済”の処理を  
終了し、設定値AMよりも少ない場合には、データリ  
プロセスにタイムアウトを生成し、データリプロセスに  
進む。

〔1268〕 また、図126から図127は、“決済”  
の処理におけるワーチャントプロセスの処理フローを示  
している。

〔1269〕 ワーチャントプロセスでは、“決済”の処  
理は、クレジット決済端末から、借用照会要求5700を受  
信することによって開始される。ワーチャントプロセス  
は、まず、スレッフ9500で、サービス提供者のグライ  
ベート間で、受信した借用照会要求の暗号を復号化し、ス  
レッフ9501で、ワーチャントプロセス有効性チェックを  
行ない、借用照会要求の有効性を検証する。

〔1270〕 ワーチャントプロセス有効性チェックにパ  
スした場合には、ワーチャントプロセスは、スレッフ95  
02で、ワーチャントプロセス管理情報のサービス・デ  
リクタプロセスIDの値から、プロセスグループに属し

ている否かを判定し、プロセスグループに属している  
場合 (サービス・デリクタプロセスID≠0) には、  
スレッフ9515で、暗号を復号化した借用照会要求を、サ  
ービス・デリクタプロセスへ送信し、プロセスグルー  
プに属していない場合 (サービス・デリクタプロセス  
ID=0) には、スレッフ9503で、暗号を復号化した借  
用照会要求を、サービス・マネージャプロセスへ送信す  
る。

〔1271〕 ワーチャントプロセス有効性チェックにフ  
ェイルした場合には、ワーチャントプロセスは、受信し  
たメッセージは有効ではないと判定し、スレッフ9514  
で、ワーチャントプロセス・セリジョン・エラー処理を  
行ない、“決済”の処理を終了する。

〔1272〕 サービス・デリクタプロセス、または、  
サービス・マネージャプロセスへ借用照会要求を送信し  
たワーチャントプロセスから、スレッフ9504で、サービ  
ス・デリクタプロセスから、借用照会応答5840を受信す  
るの待つ。サービス・デリクタプロセスから、借用  
照会応答5840を受信すると、ワーチャントプロセスは、  
スレッフ9505で、借用照会応答5840を、ワーチャント  
に対して割当てして、スレッフ9506で、借用照会応答5704を  
クレジット決済端末へ送信する。

〔1273〕 クレジット決済端末に借用照会応答5704を  
送信したワーチャントプロセスは、スレッフ9507で、ク  
レジット決済端末から決済要求5705を受信するの待つ。  
クレジット決済端末から決済要求5705を受信すると、  
ワーチャントプロセスは、スレッフ9508で、サービ  
ス提供者のグライベート間で、受信した決済要求5705の  
暗号を復号化し、スレッフ9509で、ワーチャントプロセ  
ス有効性チェックを行ない、決済要求5705の有効性を検  
証する。

〔1274〕 ワーチャントプロセス有効性チェックにパ  
スした場合には、ワーチャントプロセスは、スレッフ95  
10で、暗号を復号化した決済要求5705をサービス・デ  
リクタプロセスへ送信し、ワーチャントプロセス有効性  
チェックにフェイルした場合には、受信したメッセー  
ジは有効ではないと判定し、スレッフ9516で、ワーチャ  
ントプロセス・セリジョン・エラー処理を行ない、“決  
済”の処理を終了する。

〔1275〕 サービス・デリクタプロセスへ決済要求  
を送信したワーチャントプロセスは、スレッフ9511で、  
サービス・デリクタプロセスから、決済完了通知5917  
を受信するの待つ。サービス・デリクタプロセスか  
ら、決済完了通知5917を受信すると、ワーチャントプロ  
セスは、スレッフ9512で、決済完了通知5917をワーチャ  
ントに対して割当てし、スレッフ9513で、決済完了通知  
5708をクレジット決済端末へ送信する。

〔1276〕 クレジット決済端末に決済完了通知5708を  
送信したワーチャントプロセスは、スレッフ9500で、ク  
レジット決済端末から領収書5709を受信するの待つ。

(114)

クレジット決済端末から領収書5709を受信すると、ワ  
ーチャントプロセスは、スレッフ9601で、サービス提供者  
のグライベート間で、受信した領収書5709の暗号を復号  
化し、スレッフ9602で、ワーチャントプロセス有効性チ  
ェックを行ない、領収書5709の有効性を検証する。

〔1277〕 ワーチャントプロセス有効性チェックにパ  
スした場合には、ワーチャントプロセスは、スレッフ96  
03で、暗号を復号化した領収書5709を、サービス・デ  
リクタプロセスへ送信し、スレッフ9604で、ワーチャ  
ント・販売履歴リストと販売履歴リスト・ア  
ドレスとを更新して、“決済”の処理を終了する。

〔1278〕 ワーチャントプロセス有効性チェックにフ  
ェイルした場合には、ワーチャントプロセスは、受信し  
たメッセージは有効ではないと判定し、スレッフ9605  
で、ワーチャントプロセス・セリジョン・エラー処理を  
行ない、“決済”の処理を終了する。

〔1279〕 また、図128から図129は、“決済”  
の処理におけるバーソナル・クレジット端末の処理フロ  
ーを示している。“決済”の処理は、ユーザが支払操作  
をすると、バーソナル・クレジット端末が、決済プロセ  
スを生成することによって開始される。

〔1280〕 バーソナル・クレジット端末は、まず、ス  
レッフ9700で、ユーザが支払操作において指定した、ク  
レジットカード、支払金額、支払オフジョに基づく  
て、支払オフラー・5700を生成し、スレッフ9701で、生  
成した支払オフラーを、外部経由通信で、クレジット決済  
端末へ送信する。

〔1281〕 支払オフラーをクレジット決済端末へ送信  
したバーソナル・クレジット端末は、スレッフ9702とス  
レッフ9713とで、支払オフラー・応答5701の受信を待つ。  
スレッフ9702では、支払オフラー・応答の判定を行  
ない、スレッフ9713では、タイムアウトの判定を行な  
う。

〔1282〕 スレッフ9713のタイムアウトの判定では、  
タイムアウト時間TPOR (TPOR > 0) 以上の間、支払  
オフラー・応答を受信しない場合、バーソナル・クレジ  
ット端末はタイムアウトして、スレッフ9714で、LCDに、  
支払オフラー・応答のタイムアウト・エラーを表示して、  
“決済”の処理を終了する。

〔1283〕 支払オフラー・応答を受信した場合、バー  
ソナル・クレジット端末は、スレッフ9703で、支払オフ  
ラー・応答のサービス提供者電話番号に施されたサービス提  
供者のデジタリ署名をチェックし、この署名チェックを  
パスした場合には、スレッフ9704へ進み、フェイルした  
場合には、支払オフラー・応答は有効ではないと判定し、  
スレッフ9715で、LCDに、支払オフラー・応答のエラ  
ーを表示して、“決済”の処理を終了する。

〔1284〕 バーソナル・クレジット端末は、スレッフ  
9704で、支払オフラー・応答のランザクション番号の値  
から、クレジット決済端末へ送信した支払オフラーが、

(116)

マーチャントが取扱える内容であったか否かを判定する。支払オフアーク客のトランザクション番号がゼロでない場合、支払オフアークは、マーチャントが取扱える内容であり、バーソナル・クレジット端末は、ステップ9705へ進む。支払オフアーク客のトランザクション番号がゼロの場合、支払オフアークは、マーチャントが取扱えない内容であり、バーソナル・クレジット端末は、ステップ9716で、LCDに、支払オフアーク客のエラーを表示して、“決済”の処理を終了する。

〔1285〕バーソナル・クレジット端末は、ステップ9705で、支払オフアークの支払金額と、支払オフアーク客の請求金額とを照合し、支払金額と請求金額とが等しい場合には、ステップ9708へ進む。支払金額が、請求金額よりも大きい場合には、ステップ9708で、LCDに、図4.4 (1) に示す、支払金額を確認する画面を表示し、ステップ9707とステップ9717とで、ユーザによる確認操作を待ち、ユーザによる確認操作が行なわれると、バーソナル・クレジット端末は、ステップ9708へ進む。ステップ9707では、バーソナル・クレジット端末は、ユーザによる確認操作の判定を行ない、ステップ9717では、タイムアウトの判定を行なう。

〔1286〕ステップ9717のタイムアウトの判定では、タイムアウト時間T<sub>U40</sub> (T<sub>U40</sub> > 0) 以上の間、確認操作が行なわれない場合、バーソナル・クレジット端末はタイムアウトして、ステップ9718で、LCDに、確認操作のタイムアウト・エラーを表示して、“決済”の処理を終了する。

〔1287〕バーソナル・クレジット端末は、ステップ9708で、LCDに、“支払処理実行中”を表示し、次に、ステップ9709で、支払オフアークと支払オフアーク客とから、支払要求5703を生成し、ステップ9710で、ターミナル・ステイタスから、セッション確立状態が否かを判定し、セッション確立状態の場合には、ステップ9712で、生成した支払要求をユーザプロセッサに送信し、セッション確立状態でない場合には、ステップ9711で、セッション確立処理を行ない、ユーザ提供システムとのセッションを確立してから、ステップ9711へ進む。

〔1288〕ステップ9711のセッション確立処理では、バーソナル・クレジット端末は、支払オフアーク客のサービス提供者電話番号に電話をかけて、マーチャントのホームサービスエリアのサービス提供システムに接続する。つまり、バーソナル・クレジット端末は、“決済”の処理の際に、すでに、サービス提供システムとセッションを確立している場合には、そのサービス提供システムとの間で“決済”の処理を行ない、新たに、サービス提供システムとセッションを確立する場合には、マーチャントが所在するサービスエリアのサービス提供システムとの間で“決済”の処理を行なう。

〔1289〕支払要求を送信したバーソナル・クレジット端末は、ステップ9800とステップ9807とで、ユーザ・

ロセッサから、領収書5710を受信するのを待つ。ステップ9800では、領収書5710の受信の判定を行ない、ステップ9807では、タイムアウトの判定を行なう。

〔1290〕ステップ9807のタイムアウトの判定では、タイムアウト時間T<sub>SPR</sub> (T<sub>SPR</sub> > 0) 以上の間、領収書5710を受信しない場合、バーソナル・クレジット端末はタイムアウトして、ステップ9808で、ユーザ・タイムアウト・エラー処理を行ない、“決済”の処理を終了する。

〔1291〕領収書5710を受信した場合、バーソナル・クレジット端末は、ステップ9801で、ユーザのプライベートルームで、領収書5710の暗号を復号化し、ステップ9802で、ユーザが有効性チェックを行ない、領収書5710の有効性を検証する。

〔1292〕ユーザが有効性チェックにパスした場合に、バーソナル・クレジット端末は、ステップ9803へ進む。ユーザが有効性チェックにフェイルした場合には、バーソナル・クレジット端末は、ステップ9809で、ユーザ・セッション・エラー処理を行ない、“決済”の処理を終了する。

〔1293〕バーソナル・クレジット端末は、ステップ9803で、暗号を復号化した領収書5710を、RAMのデンプラリ領域に格納し、ステップ9804で、利用履歴リストと、利用履歴リスト・アドレスを更新して、ステップ9805で、LCDに領収書を表示する。そして、ステップ9808で、デンプラリ領域の空き容量から、データアップデート処理が必要か否かを判定し、デンプラリ領域の空き容量が、設定値AU (AU > 0) 以上ある場合には、そのまま、“決済”の処理を終了し、設定値AUよりも少ない場合には、データアップデートプロセスを生成し、データアップデート処理へ進む。

〔1294〕また、図13.0は、“決済”の処理におけるユーザプロセッサの処理フローを示している。

〔1295〕ユーザプロセッサでは、“決済”の処理は、バーソナル・クレジット端末から、支払要求5703を受信することによって開始される。ユーザプロセッサは、まず、ステップ9900で、サービス提供者のプライベートルームで、受信した支払要求の暗号を復号化し、ステップ9901で、ユーザプロセッサが有効性チェックを行ない、支払要求の有効性を検証する。

〔1296〕ユーザプロセッサが有効性チェックにパスした場合に、ユーザプロセッサは、ステップ9907で、ユーザプロセッサ管理情報のサービス・ディレクタプロセッサIDの値から、プロセッサグループに属しているか否かを判定し、プロセッサグループに属している場合 (サービス・ディレクタプロセッサID ≠ 0) には、ステップ9909で、暗号を復号化した支払要求を、サービス・ディレクタプロセッサへ送信し、プロセッサグループに属していない場合 (サービス・ディレクタプロセッサID = 0) には、ステップ9903で、暗号を復号化した支払要求を、サービス・

(116)

マネージャプロセッサへ送信する。  
〔1297〕ユーザプロセッサが有効性チェックにフェイルした場合には、ユーザプロセッサは、受信したメッセージは有効でないとして判定し、ステップ9908で、ユーザプロセッサ・セッション・エラー処理を行ない、“決済”の処理を終了する。

〔1298〕サービス・ディレクタプロセッサ、または、サービス・マネージャプロセッサへ支払要求を送信したユーザプロセッサは、ステップ9904で、サービス・マネージャプロセッサから、領収書6016を受信するのを待つ。サービス・マネージャプロセッサから、領収書6016を受信すると、ユーザプロセッサは、ステップ9905で、領収書6016をユーザ宛てに封書化して、ステップ9906で、領収書5710をバーソナル・クレジット端末へ送信し、さらに、ステップ9907で、ユーザ情報サーバ上の利用履歴リストと利用履歴リスト・アドレスとを更新して、“決済”の処理を終了する。

〔1299〕また、図13.1 (a) は、“決済”の処理における決済システムの処理フローを示している。“決済”の処理は、サービス提供システムの決済処理機関プロセッサから、決済要求5706を受信することによって開始される。

〔1300〕決済システムは、まず、ステップ10000で、決済処理機関のプライベートルームで、受信した決済要求5706の暗号を復号化し、ステップ10001で、決済処理機関が有効性チェックを行ない、決済要求5706の有効性を検証する。

〔1301〕決済処理機関が有効性チェックにパスした場合に、決済システムは、ステップ10002で、決済要求5706に基づいて、加入者情報サーバと、加盟店情報サーバと、取引情報サーバとのデータを更新して、決済処理を行ない、ステップ10003で、決済完了通知5707を生成し、ステップ10004で、生成した決済完了通知5707を決済処理機関プロセッサへ送信して、“決済”の処理を終了する。

〔1302〕決済処理機関が有効性チェックにフェイルした場合に、決済システムは、受信したメッセージは、有効なメッセージではないと判断して、ステップ10005で、決済処理機関・セッション・エラー処理を行ない、“決済”の処理を終了する。決済処理機関・セッション・エラー処理では、決済システムは、決済システムの管理システムへ、セッション・エラーメッセージを送信し、サービス提供システムの決済処理機関プロセッサにセッション・エラーメッセージを送信して、決済処理機関との回線を切断する。

〔1303〕また、決済処理機関が有効性チェックは、サービス提供システムの決済処理機関プロセッサから受信したメッセージの有効性を検証する処理であり、図13.1 (b) に示すように、決済処理機関が有効性チェックでは、4種類の検証を行なう。まず、ステップ10006で、

サービス提供者のデジタル署名を検証し、ステップ10007で、サービス提供者IDを照合し、ステップ10008で、受信したメッセージの有効期間を検証し、さらに、ステップ10009で、受信したメッセージの発行時刻を検証する。ステップ10009の発行時刻の検証では、受信した情報の発行時刻と、現在の時刻とのズレを検証し、ズレが時間T<sub>TP</sub> (T<sub>TP</sub> > 0) 以上である場合には、無効な情報であると判定する。したがって、サービス提供者のデジタル署名の検証にパスし、サービス提供者IDが一致し、有効期間の検証をパスし、発行時刻の検証にパスした場合のみ、決済処理機関が有効性チェックにパスしたと判定し、それ以外の場合は、フェイルしたと判定する。  
〔1304〕また、図13.2 (a) は、“決済”の処理における決済処理機関プロセッサの処理フローを示している。決済処理機関プロセッサでは、“決済”の処理は、サービス・ディレクタプロセッサから、決済要求5910を受信することによって開始される。

〔1305〕決済処理機関プロセッサは、まず、ステップ10100で、決済要求5910を、決済処理機関宛てに封書化して、ステップ10101で、決済要求5706を決済システムへ送信する。

〔1306〕決済システムに決済要求5706を送信した決済処理機関プロセッサは、ステップ10102で、決済システムから、決済完了通知5707を受信するのを待つ。決済システムから決済完了通知5707を受信すると、決済処理機関プロセッサは、ステップ10103で、サービス提供者のプライベートルームで、受信した決済完了通知5707の暗号を復号化し、ステップ10104で、決済処理機関プロセッサが有効性チェックを行ない、決済完了通知5707の有効性を検証する。

〔1307〕決済処理機関プロセッサが有効性チェックにパスした場合には、決済処理機関プロセッサは、ステップ10105で、暗号を復号化した決済完了通知5707を、サービス・ディレクタプロセッサへ送信し、ステップ10106で、決済処理機関情報サーバ上の決済履歴リストと決済履歴リスト・アドレスとを更新して、“決済”の処理を終了する。

〔1308〕決済処理機関プロセッサが有効性チェックにフェイルした場合には、決済処理機関プロセッサは、受信したメッセージは有効でないとして判定し、ステップ10107で、決済処理機関・セッション・エラー処理を行ない、“決済”の処理を終了する。決済処理機関・セッション・エラー処理では、決済システムとの回線は切断される。この際、決済処理機関プロセッサは、無効なメッセージを受信したことを示すセッション・エラーメッセージを、管理システム407に送信する。

〔1309〕また、決済処理機関プロセッサが有効性チェックは、決済システムから受信した情報の有効性を検証す



(117)

る処理であり、図13.2 (b) に示すように、決済処理機関フロセス有効性チェックでは、3種類の検証を行なう。まず、スレッツァ10108で、決済処理機関のデジタル署名を検証し、スレッツァ10109で、決済処理機関IDを照合し、さらに、スレッツァ10110で、受信した情報の発行時刻を検証し、スレッツァ10110の発行時刻の検証では、受信した情報の発行時刻と、現在の時刻とのズレを検証し、ズレが時間TTP (TTP > 0) 以上である場合に、無効な情報であると判定する。したがって、決済処理機関のデジタル署名の検証にパスし、決済処理機関IDが一致し、発行時刻の検証にパスした場合のみ、決済処理機関フロセス有効性チェックにパスしたと判定し、それ以外の場合は、フェイルしたと判定する。

(1310) また、図13.3から図13.4は、“決済”の処理におけるサービス・デイレクタフロセスの処理フローを示している。

(1311) サービス・デイレクタフロセスでは、サービス・マネージャフロセスから、信用照会要求5820と支払要求5827を受信した場合、または、サーチャントフロセスから、支払要求5827を受信した場合、または、サーチャントフロセスから、信用照会要求5820を受信した場合、または、ユーザフロセスから、支払要求5827を受信した場合、または、ユーザフロセスから、支払要求5827を受信する場合に、“決済”の処理を開始する。

(1312) サーチャントフロセスから、信用照会要求5820を受信した場合には、サービス・デイレクタフロセスは、スレッツァ10216で、ユーザフロセスから支払要求5827を受信するのを待ち、ユーザフロセスから支払要求5827を受信すると、スレッツァ10200へ進む。

(1313) また、ユーザフロセスから、支払要求5827を受信した場合には、サービス・デイレクタフロセスは、スレッツァ10217で、サーチャントフロセスから信用照会要求5820を受信するのを待ち、サーチャントフロセスから信用照会要求5820を受信すると、スレッツァ10200へ進む。

(1314) サービス・マネージャフロセスから、信用照会要求5820と支払要求5827を受信した場合には、サービス・デイレクタフロセスは、そのまま、スレッツァ10200へ進み、信用照会要求5820と支払要求5827との有効性をチェックする。スレッツァ10200の信用照会要求と支払要求との有効性チェックでは、サービス・デイレクタフロセスは、信用照会要求の支払オプナー及び支払オプナー応答の部分と、支払要求の支払オプナー及び支払オプナー応答の部分とのデータ照合と、その支払オプナー及び支払オプナー応答の有効期間の検証とを行ない、データ照合が一致して、有効期間の検証にパスした場合のみ、信用照会要求と支払要求の有効性チェックにパスしたと判定し、それ以外の場合は、フェイルと判定する。

(1315) 信用照会要求と支払要求の有効性チェックにフェイルした場合には、サービス・デイレクタフロセスは、スレッツァ10212で、サービス・デイレクタフロセス

ス・セッション・エラー処理を行ない、“決済”の処理を終了する。サービス・デイレクタフロセス・セッション・エラー処理によって、サービス・デイレクタフロセスと、そのサービス・デイレクタフロセスと同じフロセスグループのユーザフロセス及びサーチャントフロセスとは、サービス・マネージャフロセスによって消去される。この際、サービス・デイレクタフロセスは、無効なメッセージを受信したことを示すセッション・エラーメッセージを、管理システム401に送信する。

(1316) 信用照会要求及び支払要求の有効性チェックにパスした場合には、サービス・デイレクタフロセスは、まず、スレッツァ10201で、サーチャントの顧客データを参照して、次に、スレッツァ10202で、ユーザに対応する顧客番号を特定し、次に、スレッツァ10202で、ユーザに対応するユーザ情報サーバ上の情報にアクセスして、信用照会要求5840を生成し、スレッツァ10203で、生成した信用照会要求5840をサーチャントフロセスへ送信し、さらに、スレッツァ10204で、サービス提供履歴リスト4303に、信用照会のサービス提供履歴を追加して、サービス提供履歴リスト4303を更新する。

(1317) スレッツァ10203の信用照会要求5840の生成では、サービス・デイレクタフロセスは、ユーザの信用状況に問題がある場合に、サービス・デイレクタフロセスは、ユーザとユーザ情報サーバとの間で、以前に、バーチャル・リムーブ・クレジット決済サービスによる取引がない場合には、ユーザIDに対応する顧客番号は特定できないので、この場合は顧客番号5343は既定しない。

(1318) スレッツァ10204で、サービス提供履歴リストを更新したサービス・デイレクタフロセスは、スレッツァ10205とスレッツァ10212とで、サーチャントフロセスから、決済要求5850を受信するのを待ち、スレッツァ10205では、決済要求5850の受信の判定を行ない、スレッツァ10212では、タイムアウトの判定を行なう。

(1319) スレッツァ10212のタイムアウトの判定では、タイムアウト時間TTCR (TTCR > 0) 以上の間、決済要求5850を受信しない場合、サービス・デイレクタフロセスはタイムアウトして、スレッツァ10214で、サービス・デイレクタフロセス・タイムアウト・エラー処理を行ない、“決済”の処理を終了する。サービス・デイレクタフロセス・タイムアウト・エラー処理によって、サービス・デイレクタフロセスと、そのサービス・デイレクタフロセスと同じフロセスグループのユーザフロセス及びサーチャントフロセスとは、サービス・マネージャフロセスによって消去される。この際、サービス・デイレクタフロセスは、タイムアウトしたことを示すタイムアウト・エラーメッセージを、管理システム401に送信する。

(1320) サーチャントフロセスから決済要求5850を受信した場合は、サービス・デイレクタフロセスは、スレ

(118)

ツァ10206で、決済要求5850の有効性をチェックする。スレッツァ10206の決済要求の有効性チェックでは、サービス・デイレクタフロセスは、決済要求5850の支払オプナー及び支払オプナー応答の部分と、支払要求の支払オプナー及び支払オプナー応答の部分とのデータ照合と、決済要求5850の照会番号と信用照会要求の照会番号との照合と、決済要求5850の有効期間の検証とを行ない、データ照合が一致し、照会番号が一致して、有効期間の検証にパスした場合にのみ、決済要求の有効性チェックにパスしたと判定し、それ以外の場合は、フェイルと判定する。

(1321) 決済要求の有効性チェックにフェイルした場合には、サービス・デイレクタフロセスは、スレッツァ10215で、サービス・デイレクタフロセス・セッション・エラー処理を行ない、“決済”の処理を終了する。

(1322) 決済要求の有効性チェックにパスした場合には、サービス・デイレクタフロセスは、スレッツァ10207で、決済処理機関データファイル4304を参照して、決済処理を要求する決済処理機関を選定し、スレッツァ10208で、サービス・マネージャフロセスに、メンバーフロセス要求を送信して、同メンバーフロセスグループのメンバーフロセスとして、選定した決済処理機関に格納する決済処理機関IDを要求し、スレッツァ10209で、要求した決済処理機関フロセスが、メンバーフロセスになるのを待つ。

(1323) 要求した決済処理機関フロセスが、メンバーフロセスになると、サービス・デイレクタフロセスは、スレッツァ10210で、ユーザに対応するユーザ情報サーバ上の情報と、サーチャントに対応するサーチャント情報サーバ上の情報と、決済処理機関に格納する決済処理機関情報サーバ上の情報とにアクセスして、決済要求5910を生成し、スレッツァ10211で、生成した決済要求5910を、決済処理機関フロセスへ送信する。

(1324) 決済要求5910を送信したサービス・デイレクタフロセスは、スレッツァ10300とスレッツァ10311とで、決済処理機関フロセスから、決済完了通知5927を受信するのを待ち、スレッツァ10300では、決済完了通知5927の受信の判定を行ない、スレッツァ10311では、タイムアウトの判定を行なう。

(1325) スレッツァ10311のタイムアウトの判定では、タイムアウト時間TTPC (TTPC > 0) 以上の間、決済完了通知5927を受信しない場合、サービス・デイレクタフロセスはタイムアウトして、スレッツァ10312で、サービス・デイレクタフロセス・タイムアウト・エラー処理を行ない、“決済”の処理を終了する。

(1326) 決済処理機関フロセスから決済完了通知5927を受信した場合、サービス・デイレクタフロセスは、スレッツァ10301で、ユーザに対応する顧客番号があるかを判定し、顧客番号がある場合には、スレッツァ10303へ進み、顧客番号がない場合には、スレッツァ10307で、

サーチャントに対してユーザをユニークに示す顧客番号を生成して、サーチャントの顧客データファイルに格納してから、スレッツァ10303へ進む。

(1327) サービス・デイレクタフロセスは、スレッツァ10303で、決済完了通知5927と決済要求5850とから、サーチャントへの決済完了通知5937を生成し、スレッツァ10304で、生成した決済完了通知5937を、サーチャントフロセスへ送信する。

(1328) 決済完了通知5937を送信したサービス・デイレクタフロセスは、スレッツァ10305とスレッツァ10313とで、サーチャントフロセスから、領収書5008を受信するのを待ち、スレッツァ10305では、領収書5008の受信の判定を行ない、スレッツァ10313では、タイムアウトの判定を行なう。

(1329) スレッツァ10313のタイムアウトの判定では、タイムアウト時間TTR (TTR > 0) 以上の間、領収書5008を受信しない場合、サービス・デイレクタフロセスはタイムアウトして、スレッツァ10314で、サービス・デイレクタフロセス・タイムアウト・エラー処理を行ない、“決済”の処理を終了する。

(1330) サーチャントフロセスから領収書5008を受信した場合、サービス・デイレクタフロセスは、スレッツァ10306で、領収書5008と決済完了通知5937とから、ユーザへの領収書5016を生成し、スレッツァ10307で、生成した領収書5016を、ユーザフロセスへ送信し、スレッツァ10308で、サービス提供履歴リスト4303に、サービス提供履歴を追加して、サービス提供履歴リスト4303を更新する。

(1331) サービス提供履歴リスト4303を更新したサービス・デイレクタフロセスは、スレッツァ10309で、ユーザフロセスが“決済”の処理を完了するのを待ち、ユーザフロセスが“決済”の処理を完了すると、スレッツァ10310で、サービス・デイレクタフロセス自身のフロセス消去要求をサービス・マネージャフロセスへ送信して、“決済”の処理を終了する。スレッツァ10310のフロセス消去要求の送信によって、サービス・デイレクタフロセスは、サービス・マネージャフロセスによって消去される。

(1332) 次に、“キャンセル”の処理における処理フローについて説明する。

(1333) 図13.5は、“キャンセル”の処理におけるクレジット決済端末の処理フローを示している。“キャンセル”の処理は、サーチャントが、キャンセル操作901をすると、クレジット決済端末900が、キャンセルフロセスを生成することによって開始される。

(1334) クレジット決済端末は、まず、スレッツァ10400で、LCDに“販売キャンセル処理実行中”を表示し、スレッツァ10401で、キャンセルする取引の決済完了通知5937から、キャンセル要求6100を生成し、スレッツァ10402で、ターミナル・ステータスから、セッション番

(119)

立状態が否かを判定し、セッション確立状態の場合には、ステップ1004で、生成したキャンセル要求をマーチャントプロセスに送信し、セッション確立状態でない場合には、ステップ1003でセッション確立処理を行ない、サービス提供システムとのセッションを確立してから、ステップ1004へ進む。

[11335] キャンセル要求を送信したクレジット決済端末は、ステップ1005とステップ10412とで、マーチャントプロセスからキャンセル完了通知104を受信するのを待つ。ステップ10405では、キャンセル完了通知104の受信の判定を行ない、ステップ10412では、タイムアウトの判定を行なう。

[11336] ステップ10412のタイムアウトの判定では、タイムアウト時間TSPCC (TSPCC) 0) 以上の間、キャンセル完了通知104が受信されない場合、クレジット決済端末はタイムアウトして、ステップ10413で、マーチャント・タイムアウト・エラー処理を行ない、“キャンセル”の処理を終了する。

[11337] キャンセル完了通知104を受信した場合、クレジット決済端末は、ステップ10406で、マーチャントのプライベート鍵で、受信したキャンセル完了通知104の暗号を復号化し、ステップ10407で、マーチャントの有効性チェックを行ない、受信したメッセージの有効性を検証する。

[11338] マーチャント有効性チェックにパスした場合には、クレジット決済端末は、ステップ10408へ進む。マーチャント有効性チェックにフェイルした場合には、クレジット決済端末は、ステップ10414で、マーチャント・セッション・エラー処理を行ない、“キャンセル”の処理を終了する。

[11339] クレジット決済端末は、ステップ10408で、暗号を復号化したキャンセル完了通知104をRAMのテンポラリ領域に格納し、ステップ10409で、販売履歴リストと、販売履歴リスト・アドレスとを更新して、ステップ10410で、LCDに、キャンセル処理の完了を表示する。そして、ステップ10411で、テンポラリ領域の空き容量が、データアップデート処理が必要か否かを判定し、テンポラリ領域の空き容量が、設定値AM (AM > 0) 以上ある場合には、そのまま、“キャンセル”の処理を終了し、設定値AMより少ない場合には、データアップデートプロセスを生成し、データアップデート処理へ進む。

[11340] また、図1336は、“キャンセル”の処理におけるマーチャントプロセスの処理フローを示している。

[11341] マーチャントプロセスでは、“キャンセル”の処理は、クレジット決済端末から、キャンセル要求104を受信することによって開始される。マーチャントプロセスは、まず、ステップ10500で、サービス提供者のプライベート鍵で、受信したキャンセル要求の暗号

を復号化し、ステップ10501で、マーチャントプロセス有効性チェックを行ない、キャンセル要求の有効性を検証する。

[11342] マーチャントプロセス有効性チェックにパスした場合には、マーチャントプロセスは、ステップ10502で、マーチャントプロセス管理情報のサービス・ディレクタプロセスIDの値から、プロセスグループに属しているか否かを判定し、プロセスグループに属している場合 (サービス・ディレクタプロセスID≠0) には、ステップ10503で、暗号を復号化したキャンセル要求を、サービス・ディレクタプロセスへ送信し、プロセスグループに属していない場合 (サービス・ディレクタプロセスID=0) には、ステップ10503で、暗号を復号化したキャンセル要求を送信する。

[11343] マーチャントプロセス有効性チェックにフェイルした場合には、マーチャントプロセスは、受信したメッセージは有効ではないと判定し、ステップ10508で、マーチャントプロセス・セッション・エラー処理を行ない、“キャンセル”の処理を終了する。

[11344] サービス・ディレクタプロセス、またはサービス・マネージャプロセスへキャンセル要求105を送信したマーチャントプロセスは、ステップ10504で、サービス・ディレクタプロセスから、キャンセル完了通知104を受信するのを待つ。

[11345] サービス・ディレクタプロセスからキャンセル完了通知104を受信すると、マーチャントプロセスは、ステップ10505で、キャンセル完了通知104を、マーチャント宛てに封書化して、ステップ10506で、キャンセル完了通知104をクレジット決済端末へ送信し、ステップ10507で、マーチャント情報サーバ上の販売履歴リストと販売履歴リスト・アドレスとを更新して、“キャンセル”の処理を終了する。

[11346] また、図1337は、“キャンセル”の処理におけるパーソナル・クレジットの処理フローを示している。“キャンセル”の処理は、ユーザがキャンセル操作304をすると、パーソナル・クレジット端末が、キャンセルプロセスを生成することによって開始される。

[11347] パーソナル・クレジット端末は、まず、ステップ10600で、LCDに、“支払キャンセル処理実行中”を表示し、次に、ステップ10601で、キャンセル要求101の暗号を復号化し、ステップ10602で、暗号を復号化したキャンセル要求101の暗号を、サービス提供者のプライベート鍵で、復号化し、ステップ10603で、キャンセル完了通知103を受信するのを待つ。ステップ10604では、タイムアウトの判定を行ない、ステップ10605で、キャンセル完了通知103の受信の判定を行ない、ステップ10606で、タイムアウト・エラー処理を行ない、“キャンセル”の処理を終了する。

(120)

[11348] キャンセル要求101を送信したパーソナル・クレジット端末は、ステップ10605とステップ10612とで、ユーザプロセスから、キャンセル処理履歴105を受信するのを待つ。ステップ10605では、キャンセル処理履歴105の受信の判定を行ない、ステップ10612では、タイムアウトの判定を行なう。

[11349] ステップ10612のタイムアウトの判定では、タイムアウト時間TSPCR (TSPCR) 0) 以上の間、キャンセル処理履歴105を受信しない場合、パーソナル・クレジット端末はタイムアウトして、ステップ10613で、ユーザ・タイムアウト・エラー処理を行ない、“キャンセル”の処理を終了する。

[11350] キャンセル処理履歴105を受信した場合は、パーソナル・クレジット端末は、ステップ10606で、ユーザのプライベート鍵で、キャンセル処理履歴105の暗号を復号化し、ステップ10607で、ユーザ有効性チェックを行ない、キャンセル処理履歴105の有効性を検証する。

[11351] ユーザ有効性チェックにパスした場合には、パーソナル・クレジット端末は、ステップ10608へ進む。ユーザ有効性チェックにフェイルした場合には、パーソナル・クレジット端末は、ステップ10614で、ユーザ・セッション・エラー処理を行ない、“キャンセル”の処理を終了する。

[11352] パーソナル・クレジット端末は、ステップ10608で、暗号を復号化したキャンセル処理履歴105を、RAMのテンポラリ領域に格納し、ステップ10609で、利用履歴リストと、利用履歴リスト・アドレスとを更新して、ステップ10610で、LCDに、キャンセル処理履歴を表示する。そして、ステップ10611で、テンポラリ領域の空き容量が、データアップデート処理が必要か否かを判定し、テンポラリ領域の空き容量が、設定値AU (AU > 0) 以上ある場合には、そのまま、“キャンセル”の処理を終了し、設定値AUより少ない場合には、データアップデートプロセスを生成し、データアップデート処理へ進む。

[11353] また、図1338は、“キャンセル”の処理におけるユーザプロセスの処理フローを示している。

[11354] ユーザプロセスでは、“キャンセル”の処理は、パーソナル・クレジット端末から、キャンセル要求101を受信することによって開始される。ユーザプロセスは、まず、ステップ10700で、サービス提供者のプライベート鍵で、受信したキャンセル要求101の暗号を復号化し、ステップ10701で、ユーザプロセス有効性チェックを行ない、キャンセル要求101の有効性を検証する。

[11355] ユーザプロセス有効性チェックにパスした場合には、ユーザプロセスは、ステップ10702で、ユーザプロセス管理情報のサービス・ディレクタプロセスIDの値から、プロセスグループに属しているか否かを判

定し、プロセスグループに属している場合 (サービス・ディレクタプロセスID≠0) には、ステップ10709で、暗号を復号化したキャンセル要求101を、サービス・ディレクタプロセスへ送信し、プロセスグループに属していない場合 (サービス・ディレクタプロセスID=0) には、ステップ10709で、暗号を復号化したキャンセル要求101を、サービス・マネージャプロセスへ送信する。

[11356] ユーザプロセス有効性チェックにフェイルした場合には、ユーザプロセスは、受信したメッセージは有効ではないと判定し、ステップ10708で、ユーザプロセス・セッション・エラー処理を行ない、“キャンセル”の処理を終了する。

[11357] サービス・ディレクタプロセス、または、サービス・マネージャプロセスへキャンセル要求103を送信したユーザプロセスは、ステップ10704で、サービス・ディレクタプロセスから、キャンセル処理履歴105を受信するのを待つ。サービス・ディレクタプロセスから、キャンセル処理履歴105を受信すると、ユーザプロセスは、ステップ10705で、キャンセル処理履歴105を、ユーザ宛てに封書化して、ステップ10706で、キャンセル処理履歴105をパーソナル・クレジット端末へ送信し、さらに、ステップ10707で、ユーザ情報サーバ上の利用履歴リストと利用履歴リスト・アドレスとを更新して、“キャンセル”の処理を終了する。

[11358] また、図1339は、“キャンセル”の処理における決済システム処理フローを示している。“キャンセル”の処理は、サービス提供システムの決済処理履歴105から、キャンセル要求102を受信することによって開始される。

[11359] 決済システムは、まず、ステップ10800で、決済処理履歴のプライベート鍵で、受信したキャンセル要求102の暗号を復号化し、ステップ10801で、決済処理履歴有効性チェックを行ない、キャンセル要求102の有効性を検証する。

[11360] 決済処理履歴有効性チェックにパスした場合には、決済システムは、ステップ10802で、キャンセル要求102に基づいて、加入者情報サーバと、加盟店情報サーバと、取引情報サーバとのデータを更新して、クレジット決済処理のキャンセル処理を行ない、ステップ10803で、キャンセル完了通知103を生成し、ステップ10804で、生成したキャンセル完了通知103を、決済処理履歴105へ送信して、“キャンセル”の処理を終了する。

[11361] 決済処理履歴有効性チェックにフェイルした場合には、決済システムは、受信したメッセージは有効なメッセージではないと判断して、ステップ10805で、決済処理履歴セッション・エラー処理を行ない、“キャンセル”の処理を終了する。

[11362] また、図140は、“キャンセル”の処理





インレクタプロセスIDの値から、プロセスグループに属しているか否かを判定し、プロセスグループに属している場合(サービス・ディレクタプロセスID≠0)には、ステップ1121で、暗号を復号化した顧客サービスコール要求6300を、サービス・ディレクタプロセスへ送信し、プロセスグループに属していない場合(サービス・ディレクタプロセスID=0)には、ステップ1123で、暗号を復号化した顧客サービスコール要求6300を、サービス・マネージャプロセスへ送信する。

【1390】マーチャントプロセス有効性チェックにフ  
 ェイルした場合には、マーチャントプロセスは、受領し  
 たメッセージは有効ではないと判定し、ステップ1311  
 で、マーチャントプロセス・セッション・エラー処理を  
 行ない、「顧客サービスコール」の処理を終了する。

【1391】サービシ・ディレクタプロセス、または、サービシ・マネージャプロセスへ顧客サービスコール要求6406を送信したマーチャントプロセスは、ステップ11204で、サービシ・ディレクタプロセスから、顧客サービスコール応答6406を受信するのを待つ。

【1392】サービス・ディレクタプロセスから、顧客サービスコール応答6426を受信すると、マーチャントプロセスは、ステップ11205で、顧客サービスコール応答6426を、マーチャント宛てに封装化して、ステップ11206で、顧客サービスコール応答6303をクレジット決済端末へ送信する。

【1393】そして、ステップ1107で、顧客サービスコール応答の応答メッセージが、通話可か、通話不可かを判定し、通話可の場合は、ステップ1108で、サービス・ディレクタブロードキャストから、呼び出し応答6440を受信するのを待ち、通話不可の場合は、そのまま、「顧客サービスコール」の処理を終了する。

【1394】サーピス・ディレクタプロセスから、呼び出し応答6400を受信すると、マーチャントプロセスは、ステップ11209で、呼び出し応答6440を、マーチャントプロセスに割替化して、ステップ11210で、呼び出し応答6304にて封ジ化して、スレーブ端末へ送信して、デジタル音データ通信を行なった音報音源低価格へ移行する。

【1395】また、図144は、“顧客サービスコール”の処理におけるパーソナル・クレジット端末の処理フローを示している。“顧客サービスコール”の処理は、サービス提供システムから、顧客サービスコール8301を受信すると、パーソナル・クレジット端末が、顧客サービスコールプロセスを生成することによって開始される。

【1396】バーソナル・クレジット端末は、まず、ステップ11300で、ユーザのプライベートルームで、受領した顧客サービスコスコード6301の暗号を復号化し、ステップ11301で、ユーザが有効性チェックを行ない、顧客サービスコード6301の有効性を検証する。

【1397】ユーザ有効性チェックにパスした場合に

求6408を受信した場合、または、マーチャントプロセスから、顧客サービスコール要求6408を受信した場合に、“顧客サービスコール”の処理を開始する。

【1406】 サービス・ディレクタプロセスは、まず、ステップ11500で、マーチャントの顧客テーブルを参照して、顧客サービスコール要求の顧客番号#401に対応するユーザIDを待望し、次に、ステップ11501で、サービス・マネージャプロセスに、メンバープロセス要求を送る。そして、同一のプロセスグループのメンバープロセスとして、顧客サービスコールをするユーザに対応するユーザプロセスを要求し、ステップ11502とステップ11512とで、要求したユーザプロセスが、メンバープロセスになるのを待つ。ステップ11502では、要求したユーザプロセスがメンバープロセスになったか否かの判定を行なう。ステップ11512では、タイムアウトの判定を行なう。

【1140】ステップ1152のタイムアウトの判定では、タイムアウト時間TUPRP（TUPRP=0）以上の間、要求したユーザプロセスがメンバープロセスにならない場合、サービシ・ディレクタプロセスはタイムアウトして、ステップ1153で、応答メッセージ642が、通話不可を示す顧客サービスコール応答648を生成して、ステップ1154で、生成した顧客サービスコール応答648をマーチャントプロセスへ送信し、ステップ1155で、マーチャントプロセスが、“顧客サービスコール”の処理を終了するのを待たず、マーチャントプロセスが“顧客サービスコール”の処理を終了すると、サービシ・ディレクタプロセスは、ステップ1156で、サービシ・ディレクタプロセス自身のプロセス消去要求をサービシ・マネージャプロセスへ送信して、“顧客サービスコール”の処理を終了する、ステップ1157のプロセス消去要求の送附によって、サービシ・ディレクタプロセスは、サービシ・マネージャプロセスによって消去される。

【1408】要求したユーザプロセスが、メンバプロセスになった場合、サービシ・ディレクタプロセスは、ステップ1503で、ユーザのアクセス制御情報24005を参照して、ユーザにアクセスできるか否かを判定する。

【1409】ステップ11608の判定で、ユーザにアクセスできる場合、サービス・ディレクタプロセスは、ステップ11607で、顧客サービスコール6417を生成し、ステップ11608で、生成した顧客サービスコール6417をユーザプロセスへ送信し、さらに、ステップ11608で、応答メッセージ6422が、電話可を示す顧客サービスコール6428を生成して、ステップ11607で、生成した顧客サービスコール6428をマーマチャントプロセスへ送信する。

【1410】ステップ11503の判定で、ユーザにアクセスできない場合、サービス・ディレクタプロセスは、ステップ11513へ進み、ステップ11518からステップ11516の処理を行う。

は、バーソナル・クレジット端末は、ステップ11302で、スピーカから着信音を出し、LCDに、顧客サービスコールの着信を表示して、ステップ11303で、ユーザの電話操作を待つ。

【1398】ユーザ有効性チェックにフェイルした場合  
には、パーソナル・クレジット端末は、ステップ11307  
で、ユーザ・セッション・エラー処理を行ない、“顧客  
サービスコール”の処理を終了する。

【1399】ユーザが通話操作を行なうと、パーソナル・クレジット端末は、ステップ1304で、着信応答6303を生成し、ステップ1305で、生成した着信応答6303を、ユーザプロセッサへ送信し、さらに、ステップ1306で、LCDに、“通話中”を提示して、音声通話状態へ移行する。

【1400】音声データを暗号化して音声通話を行なう場合には、ステッパ1304で、第4応答6303を生成する際に、パーソナル・クレジット端末は、音声データ暗号鍵6432を生成して、第4応答6303に設定し、さらに、生成した音声データ暗号鍵6432を音声データ暗号鍵レジスタ(CRYP1)21613に設定して、音声データの暗号化と復号化を行なう。

【1401】また、図145は、“顧客サービスコール”の処理におけるユーザプロセスの処理フローを示している。

【1402】ユーザプロセスでは、「顧客サービスコーナー」の処理は、サービス・ディレクタプロセスから、顧客サービスコール6417を受信することによって開始される。顧客サービスコール6417を、ユーザが宛てて封書化した顧客サービスコール6417を、ユーザ・ステータスからし、次に、ステップ11401で、ユーザ・ステータスから、セッション確立状態が否かを判定し、セッション確立状態の場合には、ステップ11403で、顧客サービスコール6301をパーソナル・クレジット端末へ送信し、セッション確立状態でない場合には、ステップ11402で、セッション確立処理を行ない、パーソナル・クレジット端末とのセッションを確立してから、ステップ11403へ進む。

【1403】顧客サービスコール301を送信したユーザーは、ステップ1104で、パーソナル・クレジット端末から、着信応答303を受信するのを待ち、着信応答303を受信すると、ステップ1105で、サービス提供者のブライベート線で、受信した着信応答303の暗号を、復号化し、ステップ1106で、復号化した着信応答を、ユーザー・ディレクタプロセッサへ送信して、デジタル音サービス・ディレクタプロセッサへ移行する。

【1404】また、図146は、“顧客サービスコール”の処理におけるサービス・ディレクタプロセスの処理フローを示している。

【1405】サービス・ディレクタプロセスでは、サー  
ビス・マネージャプロセスから、顧客サービスコール受

【1411】顧客サービスコールセンターへ送付したサービス・ディレクタブレットは、ステップ1508とステップ1517とで、ユーザプロセスから、着信応答6433を受信するのを待つ。ステップ1508では、着信応答6433の受信の判定を行ない、ステップ1517では、タイムアウトの判定を行なう。

【1412】 ストップ11515のタイムアウトの判定では、タイムアウト時間TARU (TARU >0) 以上の間、着信番6433を受信しない場合、サービス、ディレクタブロードキャストはタイムアウトして、ステータス11518で、サービス・ディレクタブロードキャスト・タイムアウト・エラー処理を行ない、「顧客サービスセンター」の画面を終了する。

【1413】ユーザプロセスから、着信応答6433を受信した場合、サービス・ディレクタプロセスは、ステップ11509で、着信応答6433から、呼び出し応答6440を生成して、ステップ11510で、生成した呼び出し応答6440を、マスタントプロセスへ送信し、さらに、ステップ11511で、サービス提供履歴リスト4303に、顧客サービス履歴のサービス提供履歴を追加して、サービス提供履歴リスト4303を更新して、デジタル音声データ通信を行なう音声通話状態へ移行する。

【1414】次に、“問い合わせコール”の処理における処理フローについて説明する。

【1415】図147は、「問い合わせコール」の処理におけるパーソナル・クレジットの端処理フローを示している。「問い合わせコール」の処理は、ユーザが、問い合わせコール操作をすると、パーソナル・クレジット端末100が、問い合わせコールプロセスを生成することによって開始される。

【1416】パーソナル・クレジット端末は、まず、ステップ11600で、LCDに“接続処理実行中”を表示し、ステップ11601で、問い合わせコール要求6306を生成し、ステップ11602で、ターミナル・ステータスか、セッション確立状態を判定し、セッション確立状態の場合には、ステップ11604で、生成した問い合わせコール要求6306をユーザプロセスに送信し、セッション確立状態でない場合には、ステップ11603でセッション確立処理を行ない、サービス提供システムとのセッションを確立してから、ステップ11604へ進む。

【1417】問い合わせコール要求3306を送信したパ  
ソナル・クレジット端末は、ステッ11605とステッ11606  
1613とで、ユーザプロセスから、問い合わせコール応答  
3308を受信するのを待つ。ステッ11605では、問い合わせ  
コール応答3308の受信の判定を行なう。ステッ11606  
1613では、タイムアウトの判定を行なう。

【1418】ステップ1613のタイムアウトの判定では、タイムアウト時間TICR (TICR >0) 以上の間、西い合わせコール応答308が受信されない場合、バージョン・クレジット始末はタイムアウトして、ステップ1614で、ユーザ・タイムアウト・エラー処理を行ない、



09で、サービス提供履歴リスト4303に、問い合わせコードのサービス提供履歴を追加して、サービス提供履歴リスト4303を更新して、デジタル音声データ通信を行なう音声履歴状態へ移行する。

【1447】次に、ユーザが、ユーザのホームサービスエリア、または、ホームサービスエリア以外のサービスエリアで、パーソナル・リモート・クレジット決済サービスを利用する場合の動作について説明する。

【1448】図152(a)は、ユーザが、ホームサービスエリアが同じマーチャントと、ホームサービスエリアで、“決済”の処理、または、“キャンセル”の処理を行なう場合の動作を示している。

【1449】この場合、パーソナル・クレジット端末100と、クレジット決済端末300とは、ホームサービスエリア(サービスエリア112100)のサービス提供システム102と通信をして、“決済”の処理、または、“キャンセル”の処理を行なう。

【1450】サービス提供システム102では、サービス・マネージャプロセス23800が、サービス提供システム102のサービスサーバ上に、ユーザプロセス23802と、マーチャントプロセス23803と、サービスディレクタプロセス23801と、サービスディレクタプロセス23802と、サービスディレクタプロセス23803と、サービスディレクタプロセス23804とが連携して、“決済”の処理、または、“キャンセル”の処理を行なう。

【1451】また、図152(b)は、ユーザが、ホームサービスエリアが異なるマーチャントと、マーチャントのホームサービスエリアで、“決済”の処理、または、“キャンセル”の処理を行なう場合の動作を示している。

【1452】この場合、パーソナル・クレジット端末100と、クレジット決済端末300とは、マーチャントのホームサービスエリア(サービスエリア112100)のサービス提供システム102と通信をして、“決済”の処理、または、“キャンセル”の処理を行なう。

【1453】サービス提供システム102では、サービス・マネージャプロセス23800が、サービス提供システム102のサービスサーバ上に、モバイルユーザプロセス12105と、マーチャントプロセス23803と、サービスディレクタプロセス23801と、決済処理機構図プロセス23804とを生成し、一方、ユーザのホームサービスエリア(サービスエリア212101)のサービス提供システム12103が、サービス提供システム12102のサービスサーバ上に、ホームユーザプロセス23801と、ホームユーザプロセス23802と、モバイルユーザプロセス23803と、決済処理機構図プロセス23804とが連携して、“決済”の処理、または、“キャンセル”の処理を行なう。

4) のサービス提供システム12206と通信をし、クレジット決済端末300は、マーチャントのホームサービスエリア(サービスエリア112200)のサービス提供システム102と通信をして、“キャンセル”の処理を行なう。

【1461】サービス提供システム12206では、サービス・マネージャプロセス12208が、サービス提供システム12206のサービスサーバ上に、モバイルユーザプロセス12211を生成し、一方、ユーザのホームサービスエリア(サービスエリア312205)のサービス提供システム12207では、サービス・マネージャプロセス12209が、サービス提供システム12207のサービスサーバ上に、ホームユーザプロセス12210を生成し、さらに、サービス提供システム102では、サービス・マネージャプロセス23800が、サービス提供システム102のサービスサーバ上に、マーチャントプロセス23803と、サービスディレクタプロセス23801と、決済処理機構図プロセス23804とを生成して、生成されたサービスディレクタプロセス23801と、ホームユーザプロセス12210と、モバイルユーザプロセス12211と、マーチャントプロセス23803と、決済処理機構図プロセス23804とが連携して“キャンセル”の処理を行なう。

【1462】ホームユーザプロセス12210は、サービス・マネージャプロセス12208が、モバイルユーザプロセス12211を生成する際に、サービス・マネージャプロセス12209に対して、ユーザに対応するホームユーザプロセスの生成を要求するメッセージを送信することによって生成され、ホームユーザプロセス12210が生成できなかった場合(例：すでに、ユーザに対応するユーザプロセスが生成されていた場合)には、モバイルユーザプロセス12211は、生成されない。

【1463】モバイルユーザプロセス12211からサービス・マネージャプロセス12208へ送信されたキャンセル要求6218は、サービス・マネージャプロセス12208によって、サービス・マネージャプロセス23800へ送信されて、サービス・マネージャプロセス23803からサービス・マネージャプロセス23800へ送信されたキャンセル要求6205と、マーチャントプロセス23803からサービス・マネージャプロセス23801へ送信されたキャンセル要求6205とを照合されて、サービスディレクタプロセス23801と、モバイルユーザプロセス12211と、マーチャントプロセス23803と、決済処理機構図プロセス23804とによるグループが生成される。

【1464】また、図154(a)は、ホームサービスエリアが同じユーザとマーチャントの間で、“顧客サービスコール”の処理、または、“問い合わせコール”の処理を行なう場合の動作を示している。

【1465】この場合、パーソナル・クレジット端末100と、クレジット決済端末300とは、ホームサービスエリア(サービスエリア112300)のサービス提供システム102と通信をして、“顧客サービスコール”の処理、または、“問い合わせコール”の処理を行なう。

【1466】サービス提供システム102では、サービス・マネージャプロセス23800が、サービス提供システム102のサービスサーバ上に、ユーザプロセス23802と、マーチャントプロセス23803と、サービスディレクタプロセス23801と、サービスディレクタプロセス23802と、サービスディレクタプロセス23803と、サービスディレクタプロセス23804とが連携して、“顧客サービスコール”の処理、または、“問い合わせコール”の処理を行なう。

・マネージャプロセス23900が、サービス提供システム102のサービスサーバ上に、ユーザプロセス23802と、マーチャントプロセス23803と、サービスディレクタプロセス23901とを生成し、生成されたサービスディレクタプロセス23901と、ユーザプロセス23802と、マーチャントプロセス23803とが連携して、“顧客サービスコール”の処理、または、“問い合わせコール”の処理を行なう。

【1467】また、図154(b)は、マーチャントが、ホームサービスエリアが異なるユーザとの間で、“顧客サービスコール”の処理を行なう場合の動作を示している。

この場合、パーソナル・クレジット端末100は、ユーザのホームサービスエリア(サービスエリア212301)のサービス提供システム12302と通信をし、クレジット決済端末300は、マーチャントのホームサービスエリア(サービスエリア112300)のサービス提供システム102と通信をして、“顧客サービスコール”の処理を行なう。

【1468】サービス提供システム102では、サービス・マネージャプロセス23800が、サービス提供システム102のサービスサーバ上に、マーチャントプロセス23803と、サービスディレクタプロセス23801とを生成し、一方、サービス提供システム12302では、サービス・マネージャプロセス12303が、サービス提供システム12302のサービスサーバ上に、ユーザプロセス23802を生成して、生成されたサービスディレクタプロセス23801と、ユーザプロセス23802と、マーチャントプロセス23803とが連携して、“顧客サービスコール”の処理を行なう。

【1469】ユーザのホームサービスエリアのサービス提供システム12303のユーザプロセス23802は、サービスディレクタプロセス23801からメンバープロセス23800が、サービス・マネージャプロセス23803からサービス・マネージャプロセス23800が、サービス・マネージャプロセス12303に対して、ユーザに対応するユーザプロセスの生成を要求するメッセージを送信することによって生成される。

【1470】また、図155(a)は、ユーザのホームサービスエリアから、ユーザが、ホームサービスエリアが異なるマーチャントとの間で、“問い合わせコール”の処理を行なう場合の動作を示している。

【1471】この場合、パーソナル・クレジット端末100は、ユーザのホームサービスエリア(サービスエリア212401)のサービス提供システム12402と通信をし、クレジット決済端末300は、マーチャントのホームサービスエリア(サービスエリア112400)のサービス提供システム102と通信をして、“問い合わせコール”の処理を行なう。

【1472】サービス提供システム12402では、サービス・マネージャプロセス12403が、サービス提供システム12403のサービスサーバ上に、ユーザプロセス23802を生成し、一方、サービス提供システム102では、サービス・マネージャプロセス23800が、サービス提供システム102のサービスサーバ上に、ユーザプロセス23802と、マーチャントプロセス23803と、サービスディレクタプロセス23801と、サービスディレクタプロセス23802と、サービスディレクタプロセス23803と、サービスディレクタプロセス23804とが連携して、“顧客サービスコール”の処理、または、“問い合わせコール”の処理を行なう。

△102のサード・エクス・パルティに、マーズ・エントプロセス13803に、サード・エクス・パルティ・エントプロセス13804と生成し、生成されたサード・エクス・パルティ・エントプロセス13801と、マーズ・エントプロセス13802と、マーズ・エントプロセス13803とが連鎖する、「問い合わせプロセス」の処理を行なう。

（1473）マーズ・エントプロセス13803からサード・エクス・パルティ・エントプロセス1203へ送附された問い合わせコール要求5606は、サード・エクス・パルティ・エントプロセス1203によって、サード・エクス・パルティ・エントプロセス13800へ送附され、サード・エクス・パルティ・エントプロセス13801と、マーズ・エントプロセス13802と、マーズ・エントプロセス13803とを生成するプロセスが生成される。

(1474) また、図155(b)は、ユーザまたはチャントのホームサードスエリア以外のサードスエリアから、ユーザが、ホームサードスエリアが属するチャントとの間で“問い合わせコール”の処理を行なう場合の動作を示している。

【1475】この場合、パーソナルクレジット額を100は、両者のサードピアリア(サードピアリ)と1840のサードピアリステム1806と通信し、クレジット決済端末300は、マージョントのホームサードピアリア(サードピアリ)118400のサードピアリステム102と通信をして、“問い合わせコール”の処理を行なう。

【1476】 サービス提供システム2106では、サービス・データベース2103から、サービス提供システム2106のサービス・サーバ上に、モバイル・サブプロセッサ2111を生成し、一方、ユーザのホーム・サービスエリア（サービスエリア3 1305）のサービス提供システム13407と、サービス・サブ・ジャワラセシステム13409A、サービス・サブ・ジャワラセシステム134107のサービス・サーバ上に、ホーム・サブ・ジャワラセシステム102では、サービス・データベース2103から、サービス提供システム102のサービス・サーバ上に、サービス提供システム102のサービス・サブ・ジャワラセシステム213801とを生成して、生成されたサービス・サブ・ジャワラセシステム213801と、ホーム・サブ・ジャワラセシステム13411と、モバイル・サブ・ジャワラセシステム13411と、サービス・サブ・ジャワラセシステム213803とが連携し、「問い合わせコール」の処理を行なう。

〔1477〕ホムユージアロセスは1410が、サービス・アパニ・サアロセスは1408が、モバイル・ユージアロセス・1211を生産する際に、サービス・アパニ・サアロセスは1409に對して、ユージアに對するホムユージアロセスの生産を放棄するメッセージを送信することによつて生成され、ホムユージアロセスは1410が、生成できなかつた場合（例：すなはち、ユージアに對するユージアロセスが生成されるに對して）には、モバイル・ユージアロセス1211は、生成されない。

ス・サネジャ・プロセスは、3308へ送信された問い合わせ  
コール要求65056は、サービス・サネジャ・プロセスは、3344  
から、サービス・サネジャ・プロセスは、33800へ送信さ  
れる、サービス・サネジャ・プロセスは、33801と、主/パ  
ーサ・プロセスは、33411と、サーチャント・プロセスは、33803  
によるプロセス・グループが生成される。

第100と、クレジット決済機101と、サーバー提供システム102と、決済システム103とが動作することによって、パーソナル・リモート・クレジット決済サービスが提供される。ユーザは、パーソナル・リモート・クレジット決済サービスが提供されている地域であれば、どこでも、同じ内容のクレジット・リモート・クレジット決済サービスを受けることができる。

【1480】なお、パーソナル・クレジット増100に

上に、CPUバスに実行するプログラムや、サービスバスに  
 対してROMバス、及びEEPROMバスを設けて、ROMバス  
 供給の公開線路を格納するメモリデバイスとして、強誘電性  
 体不揮発性メモリを用いてもよい。強誘電体不揮発性性  
 モニタは、EEPROMやフラッシュメモリのように、書き  
 き込みが可能でありながら、バッチリなしなは、データ  
 が保持できる。しかも、EEPROMやフラッシュメモリ  
 に比べ、リーク電流の速度が高速で、しかも、低消費  
 電力という特性を持つメモリデバイスである。

に、強誘電体不揮発性メモリを用いた場合、例えば、14811) ROMIS01 及び、EEPROM15030等) わりには、データブッファ処理と同様の処理によって、ノーンナル、クレジット増減100のアログラムの大幅なパフォーマンスアップや、定期的なサービス提供者の公開更新を、比較的、短時間に、しかも、バッチリとの処理を、さばり捌くことなく、行なえるという利点がある。

【1462】また、CPU1500が処理するデータ、及びCPU500が処理するデータを格納するデータ、そして、強制電源切断発生メモリを用いてもよい、この場合、バッテリーが切れても、データが保持されるので、データバックアップ処理をする必要がなく、また、RAMのデータ保持のための電流の必要がないので、バッテリー、リチウム電池の消費電力を抑えられるとい、メリットがある。

【1483】以上の説明では、パーソナル・リモート・クレジット決済システムを構成するパーソナル・クレジット決済システムとは、パーソナル・クレジット決済システムにおける、パーソナル・クレジット決済サービスにおける、それぞれの機能を整理するための、最適なハンドウエア構成(またはソフトウェア構成)と、外部通信機能、ディスプレイ・キーボード(または、ペン入力デバイス)、マウス、プリンターを備えたコンピュータによって構成されてもよい。

0. まは、クレジットカード決済装置101の内蔵のハードウェアの、機能的に対応するハードウェアをコンパイルして、  
が備わっていないハードウェア (例：チートコーディング、  
暗号処理プロセッサ、制御ロジック部、など) に関連して、RC  
は、その機能をソフトウェア・プログラム化して、RC  
M150 (2320) に格納されているプログラムと共に、ソフ  
トウェアのOS (Operating System) 上で動作するソフト  
ウェア、プログラムに変換し、そのソフトウェア・プロ  
グラムを、コンピュータから実行可能な場所 (例：ハード  
ディスク) に格納しておく。

(1485)

(保明の効果) 以上の説明から明らかなように、本発明のパーソナル電子決済システムは、支払手段、請求手段及び貸付手段の各々が、貸付手段及び請求手段の各々の系統の通信手段を持ち、支払手段、請求手段及び貸付手段の各々の間に於ける不正な請求や個人情報等の漏洩を防ぐことができ、また、決済に必要な情報が通信手段を通じて交換されるため、販売の効率化を図ることができらる。

【1486】また、変払手段と請求手段との間では請求光などの光を用いた無線通信手段を用い、文払手段とは清算手段（またはサービスマン提供手段）との間ではラジオや無線通信手段を用いることによって、使用環境に適したミクスチュム形態を取ることができる。

【1487】を送り、支払手段から請求手段に支払請求メッセージを送り、請求手段から請求手段に支払請求メッセージを送り、請求手段及び支払手段が、これらに受領したメッセージから得た情報を含めて決済要求メッセージを生成して決済手段（またはサードパーティ提供手段）に送信し、決済手段（またはサードパーティ提供手段）がこれらの要求メッセージを照合すると共に、請求手段の不正請求や、支払手段の支払のこまくりを防ぐことができ、また、支払手段の識別番号や支払手段の所有者の電話番号などを請求手段に知られることができ、決済を受けることができる。

【148】また、一つの支払手段で、支払方法を債権の中心から選択することができないため、何枚ものクレジットカード（1489）または持ち歩く必要がある。

【149】また、支払手段及び請求手段が保持してあるデータは、決済手段（またはサードスプロバイダ手段）のデータを通じて、データの小売店によって、データのバッキングアップが可能なこと、また、支払手段及び請求手段の小売店に送ることとなる。

【1490】また、支払手段及び請求手段が保持しているデータを、アッパデータ処理することで、支払手段が蓄積されるデータと決済手段（またはサービスマ提供手段）に蓄積されるデータとの一貫性を保つことができ、

手段に最近のデータを蓄積し、それを更新することにより、支払手段及び請求手段のアクセシ時間を短くすることができるとができる。

〔1491〕また、フツプデータ処理に際して、支払手段または請求手段に蓄積されたデータの改ざんを見つけることができ、不正を防止できる。

〔1492〕また、このシステムでは、決済の取り消し

を簡単に実行することができる。また、請求手段の担当者、電話番号を知らなくとも、支払いを行なう支払手段の所有者と連絡をとることができる。また、同様に、支払手段の所有者も、電話番号を知らなくとも、請求手段の担当者と連絡をとることができる。そのため、支払手段の所有者のプライバシーを保護しながら、円滑な商取引を行なうことが可能である。

【図面の簡単な説明】

【図1】本発明の第1、第2の実施の形態におけるパーソナル電子決済システムのブロック構成図、

【図2】本発明の第1、第2の実施の形態におけるパーソナル・クレンジット端末の概略図。

【図3】本発明の第1、第2の実施の形態におけるクレ  
ジット決済端末の概観図、

【図4】本発明の第1、第2の実施の形態におけるサーバ提供システムのブロック構成図。

【図5】本発明の第1、第2の実施の形態における決壊システムのブロック構成図。

【図6】本発明の第1の実施の形態における“決済”の処理フロー図、

【図7】本発明の第1の実施の形態における“決済”の処理の際にパーソナル・コンピュータ端末のLCDに表示

される画面の模式図 (a) ~ (h) .

処理の際にクレンジットは終端のLCDに表示される面  
の模式図 (a) ~ (g) 、

【図9】本発明の第1、第2の実施の形態における“キヤンセル”の処理フロー図、

【図10】本発明の第1、第2の実施の形態における“キヤンセル”の処理の際にパーソナル・クレジット域

末のLCDに表示される画面の模式図(a)~(e)、  
【図11】本発明の第1、第2の実施の形態における

“キャンセル”の処理の際にクレジット決済端末のLCCに表示される画面の様式図 (a) ~ (g)。

【図12】(a) 本発明の第1の実施の形態における“顧客サービスコール”の処理フロー図、(b) 本発明

の第1の実施形態における“問い合わせコール”の処理フロー図

【図13】本発明の第1、第2の実施の形態における“顧客サービスコール”の処理の図にパーソナル・クロ

シット端末のLCDに表示される画面の模式図 (a)

(131)

セコール”の処理の際にパーソナル・クレジットの端末のL CDに示される画面の構成図 (h) と、前記“問い合わせコール”の処理の際にパーソナル・クレジットの端末のL CDに示される画面の構成図 (c) ~ (i) 、  
 【図14】 本発明の第1、第2の実施の形態における“顧客サービスコール”の処理の際にクレジット決済端末のL CDに示される画面の構成図 (a) ~ (e) 及び“問い合わせコール”の処理の際にクレジット決済端末のL CDに示される画面の構成図 (f) と、前記“問い合わせコール”の処理の際にクレジット決済端末のL CDに示される画面の構成図 (h) 、  
 【図15】 (a) 本発明の第1、第2の実施の形態におけるパーソナル・クレジットの端末のブロック構成図、(b) 本発明の第1、第2の実施の形態におけるパーソナル・クレジットの端末の内部レジスタの構成図、  
 【図16】 本発明の第1の実施の形態におけるパーソナル・クレジットの端末のRAMマップの構成図、  
 【図17】 本発明の第1の実施の形態におけるパーソナル・クレジットの端末のサービスデータ領域に格納されるデータの構成図、  
 【図18】 (a) 本発明の第1の実施の形態におけるパーソナル・クレジットの端末の内部レジスタの構成図、(b) 本発明の第1の実施の形態におけるパーソナル・クレジットの端末の内部レジスタのビットフィールド構成図、(c) 本発明の第1の実施の形態におけるパーソナル・クレジットの端末のRAM上の変数interruptのビットフィールド構成図、  
 【図19】 本発明の第1の実施の形態におけるパーソナル・クレジットの端末のCPUが行なう処理フロー図、  
 【図20】 (a) 本発明の第1の実施の形態におけるデジタル署名の処理のフロー図、(b) 本発明の第1の実施の形態におけるデジタル署名の処理のフロー図、  
 【図21】 (a) 本発明の第1の実施の形態におけるメッセージの封装化処理のフロー図、(b) 本発明の第1の実施の形態におけるメッセージの封装化処理のフロー図、  
 【図22】 (a) 本発明の第1の実施の形態における封装化されたメッセージの復号化処理のフロー図、(b) 本発明の第1の実施の形態における封装化されたメッセージの復号化処理のフロー図、  
 【図23】 (a) 本発明の第1の実施の形態におけるデジタル署名の検証処理のフロー図、(b) 本発明の第1の実施の形態におけるデジタル署名の検証処理のフロー図、  
 【図24】 (a) 本発明の第1の実施の形態におけるクレジット決済端末のブロック構成図、(b) 本発明の第1の実施の形態におけるクレジット決済端末の赤外線受発光モジュールのブロック構成図、

(132)

【図25】 本発明の第1の実施の形態におけるクレジット決済端末のRAMマップの構成図、  
 【図26】 本発明の第1の実施の形態におけるクレジット決済端末のサービスデータ領域に格納されるデータの構成図、  
 【図27】 (a) 本発明の第1の実施の形態におけるクレジット決済端末の内部レジスタの構成図、(b) 本発明の第1の実施の形態におけるクレジット決済端末の内部レジスタのビットフィールド構成図、(c) 本発明の第1の実施の形態におけるクレジット決済端末のRAM上の変数interruptのビットフィールド構成図、  
 【図28】 本発明の第1の実施の形態におけるクレジット決済端末のCPUが行なう処理のフロー図、  
 【図29】 本発明の第1の実施の形態におけるサービス提供システムユーザ情報サーバに、一人のユーザに対して格納されるデータの構成図、  
 【図30】 本発明の第1の実施の形態におけるサービス提供システムのマスタ情報サーバに、一つのマスタ情報に対して格納されるデータの構成図、  
 【図31】 本発明の第1の実施の形態におけるサービス提供システムの情報処理情報サーバに、一つの決済処理情報に対して格納されるデータの構成図、  
 【図32】 本発明の第1の実施の形態におけるサービス提供システムのサービスディレクトリ情報サーバに格納されるデータの構成図、  
 【図33】 (a) 本発明の第1の実施の形態におけるリモートアクセス処理のフロー図、(b) 本発明の第1の実施の形態におけるデータアップロード処理のフロー図、  
 【図34】 (a) 本発明の第1の実施の形態におけるリモートアクセス要求のデータ構造の構成図、(b) 本発明の第1の実施の形態におけるリモートアクセスデータのデータ構造の構成図、(c) 本発明の第1の実施の形態におけるデータアップロード要求のデータ構造の構成図、(d) 本発明の第1の実施の形態におけるデータアップロード要求のデータ構造の構成図、(e) 本発明の第1の実施の形態におけるデータアップロード要求のデータ構造の構成図、(f) 本発明の第1の実施の形態におけるデータアップロード要求のデータ構造の構成図、  
 【図35】 (a) 本発明の第1の実施の形態におけるデータアップロード要求のデータ構造の構成図、(b) 本発明の第1の実施の形態におけるデータアップロード要求のデータ構造の構成図、(c) 本発明の第1の実施の形態におけるデータアップロード要求のデータ構造の構成図、(d) 本発明の第1の実施の形態におけるデータアップロード要求のデータ構造の構成図、(e) 本発明の第1の実施の形態におけるデータアップロード要求のデータ構造の構成図、(f) 本発明の第1の実施の形態におけるデータアップロード要求のデータ構造の構成図、  
 【図36】 (a) 本発明の第1の実施の形態における支払オフラインのデータ構造の構成図、(b) 本発明の第1の実施の形態における支払オフラインのデータ構造の構成図、(c) 本発明の第1の実施の形態における支払オフラインのデータ構造の構成図、(d) 本発明の第1の実施の形態における支払オフラインのデータ構造の構成図、(e) 本発明の第1の実施の形態における支払オフラインのデータ構造の構成図、(f) 本発明の第1の実施の形態における支払オフラインのデータ構造の構成図、  
 【図37】 (a) 本発明の第1の実施の形態におけるサービス提供システムから決済システムに送信される決済要求のデータ構造の構成図、(b) 本発明の第1の実施の形態におけるサービス提供システムから決済システムに送信される決済要求のデータ構造の構成図、(c) 本発明の第1の実施の形態におけるサービス提供システムから決済システムに送信される決済要求のデータ構造の構成図、(d) 本発明の第1の実施の形態におけるサービス提供システムから決済システムに送信される決済要求のデータ構造の構成図、(e) 本発明の第1の実施の形態におけるサービス提供システムから決済システムに送信される決済要求のデータ構造の構成図、(f) 本発明の第1の実施の形態におけるサービス提供システムから決済システムに送信される決済要求のデータ構造の構成図、(g) 本発明の第1の実施の形態におけるサービス提供システムから決済システムに送信される決済要求のデータ構造の構成図、(h) 本発明の第1の実施の形態におけるサービス提供システムから決済システムに送信される決済要求のデータ構造の構成図、(i) 本発明の第1の実施の形態におけるサービス提供システムから決済システムに送信される決済要求のデータ構造の構成図、

【図42】 従来の決済システムCのブロック構成図、  
 【図43】 本発明の第2の実施の形態における“決済”の処理フロー図、  
 【図44】 前記“決済”の処理の際にパーソナル・クレジットの端末のL CDに示される画面の構成図 (a) ~ (h) 、  
 【図45】 (a) 本発明の第2の実施の形態における“顧客サービスコール”の処理フロー図、(b) 本発明の第2の実施の形態における“問い合わせコール”の処理フロー図、  
 【図46】 本発明の第2の実施の形態におけるパーソナル・クレジットの端末の内部レジスタの構成図、  
 【図47】 (a) 本発明の第2の実施の形態におけるパーソナル・クレジットの端末の内部レジスタのビットフィールド構成図、(b) 本発明の第2の実施の形態におけるパーソナル・クレジットの端末のRAM上の変数interruptのビットフィールド構成図、  
 【図48】 本発明の第2の実施の形態におけるパーソナル・クレジットの端末のRAMマップの構成図、  
 【図49】 本発明の第2の実施の形態におけるパーソナル・クレジットの端末のサービスデータ領域に格納されるデータの構成図、  
 【図50】 (a) 本発明の第2の実施の形態におけるパーソナル・クレジットの端末のCPUのプロセス一覧図、(b) 本発明の第2の実施の形態におけるパーソナル・クレジットの端末のサービス管理プロセスによるプロセスリストの更新を説明するための解説図、  
 【図51】 本発明の第2の実施の形態におけるパーソナル・クレジットの端末のCPUが行なう処理フロー図、  
 【図52】 (a) 本発明の第2の実施の形態におけるパーソナル・クレジットの端末及びクレジット決済端末のC PUが行なう処理フロー図、(b) 本発明の第2の実施の形態におけるパーソナル・クレジットの端末及びクレジット決済端末のC PUが行なう処理フロー図、(c) 本発明の第2の実施の形態におけるパーソナル・クレジットの端末及びクレジットの端末のC PUが行なう処理フロー図、  
 【図53】 本発明の第2の実施の形態におけるパーソナル・クレジットの端末のC PUが行なう処理フロー図、  
 【図54】 本発明の第2の実施の形態におけるパーソナル・クレジットの端末のC PUが行なう“決済”の処理時の処理フロー図、  
 【図55】 (a) 本発明の第2の実施の形態におけるクレジット決済端末のブロック構成図、(b) 本発明の第2の実施の形態におけるクレジット決済端末の赤外線受発光モジュールのブロック構成図、  
 【図56】 本発明の第2の実施の形態におけるクレジット決済端末のブロック構成図、







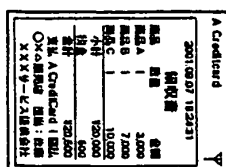




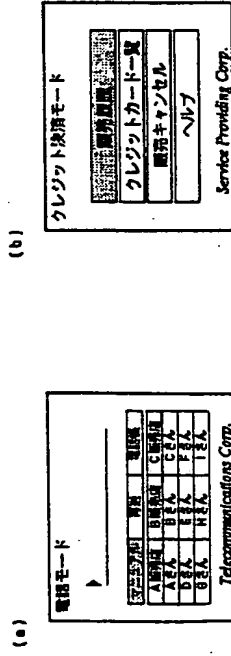


(142)

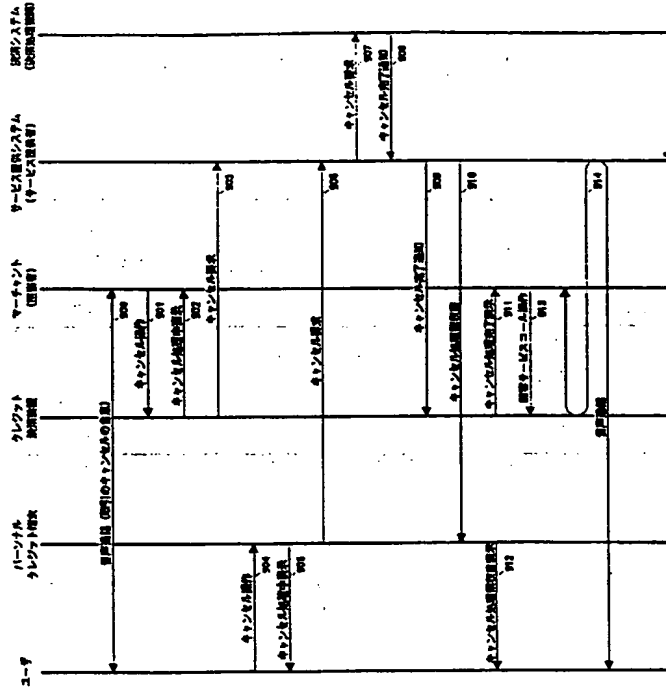
【圖 7】



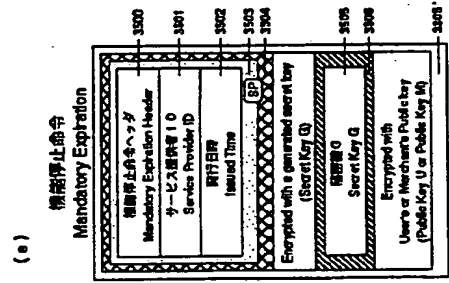
**【8圖】**



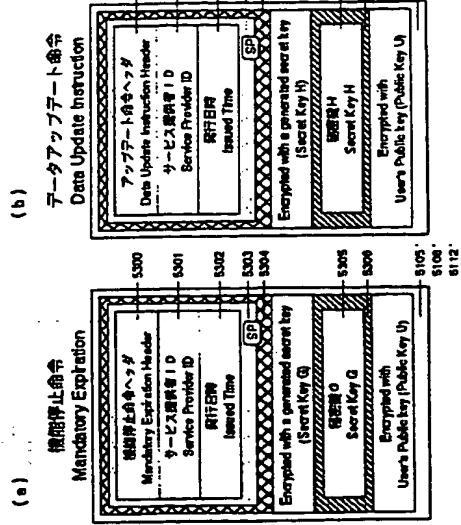
**【圖9】**



[35]



【圖84】

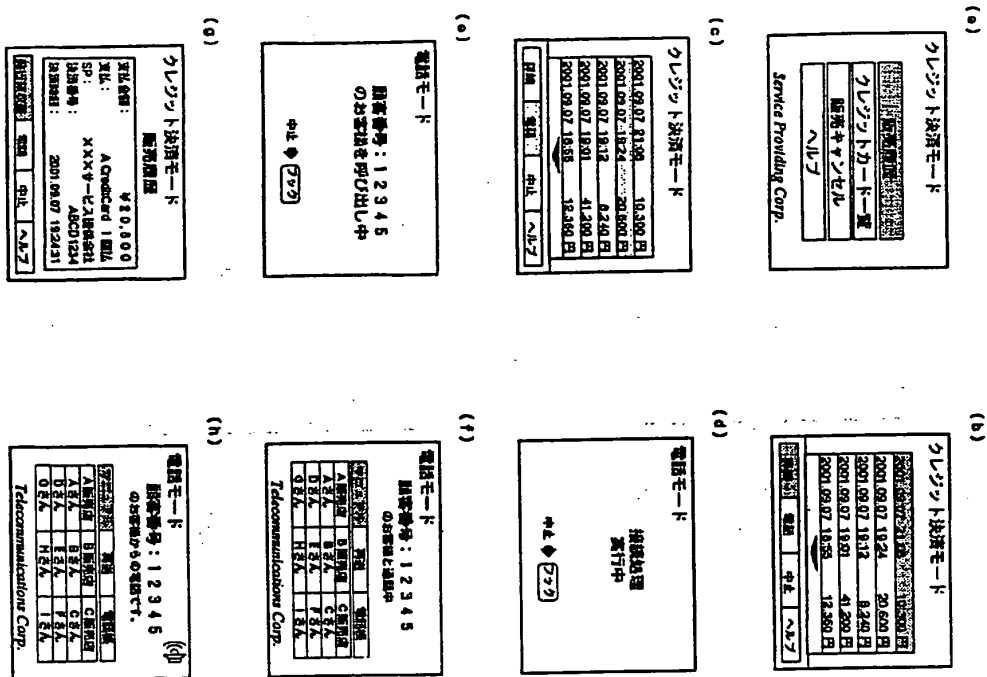






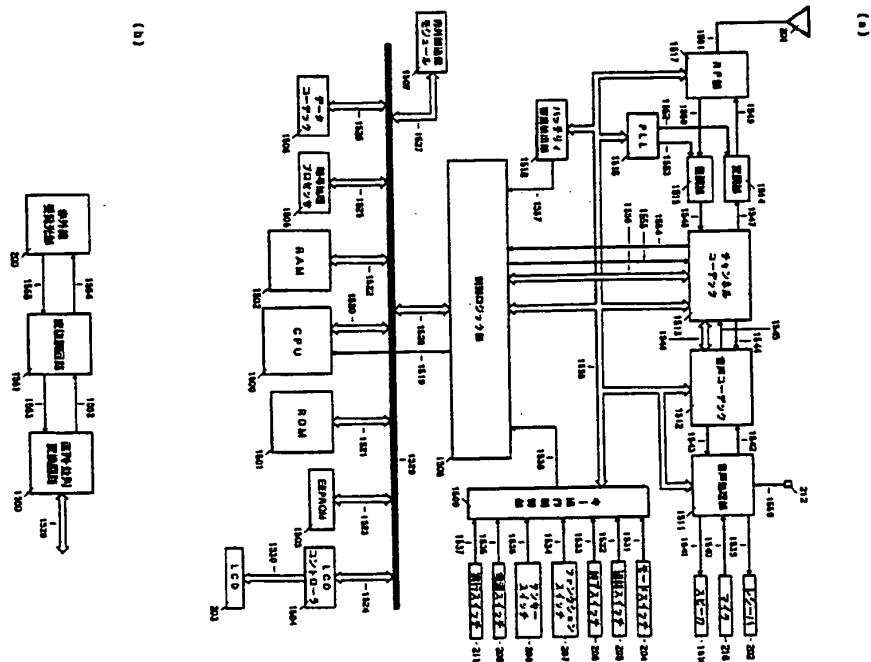
(149)

【図14】



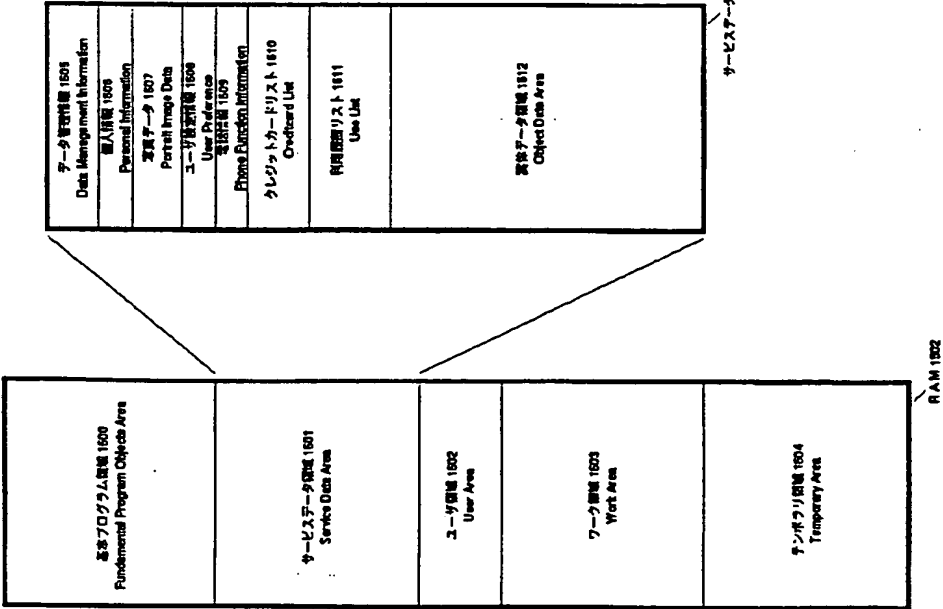
(150)

【図15】



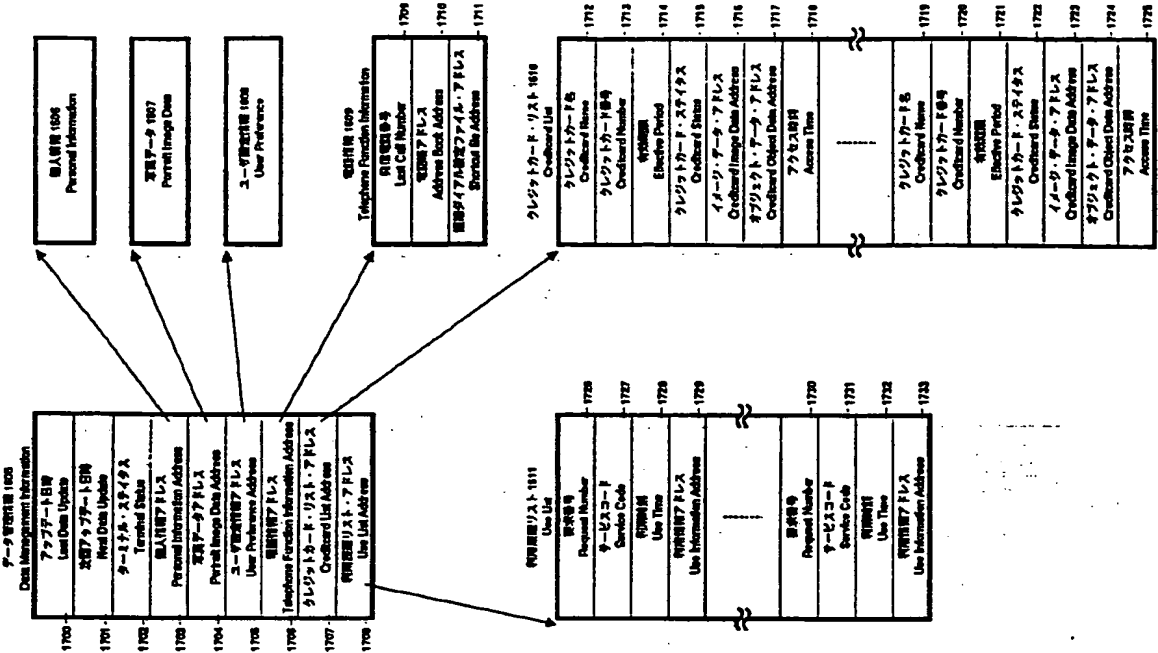
(151)

【図16】



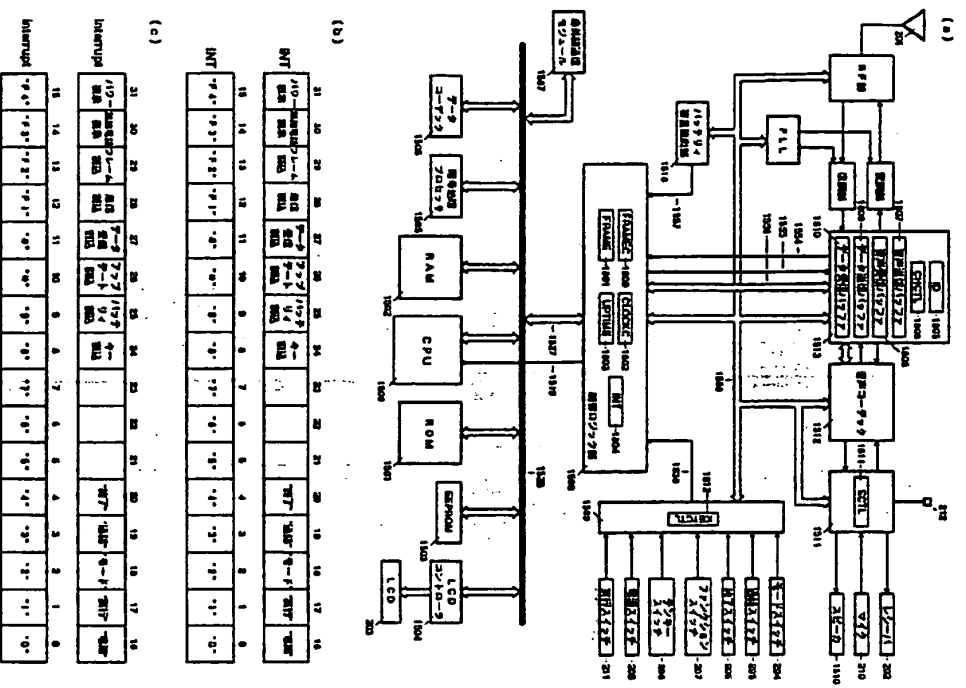
(152)

【図17】

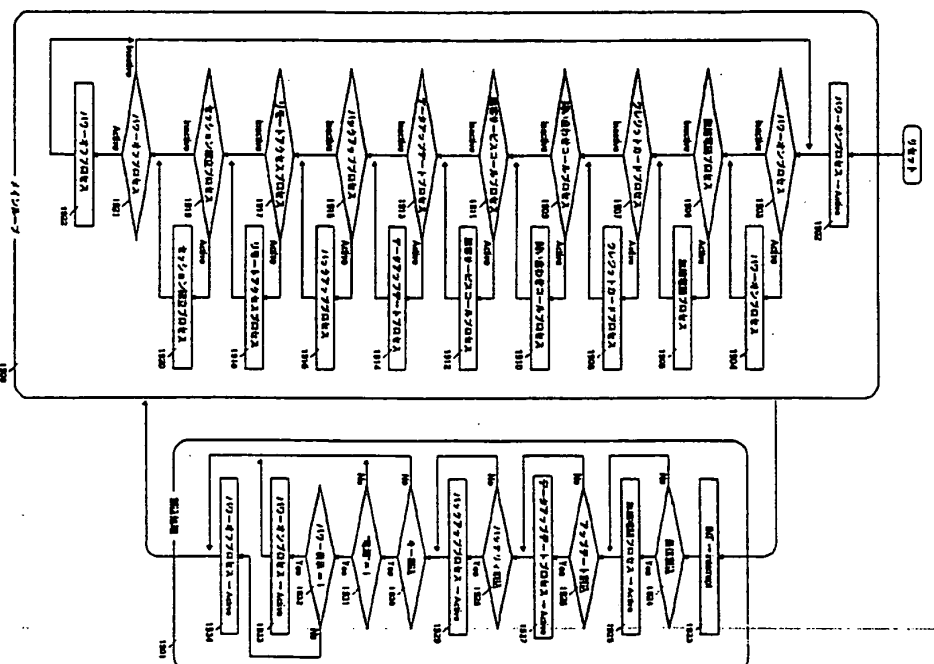




【図18】

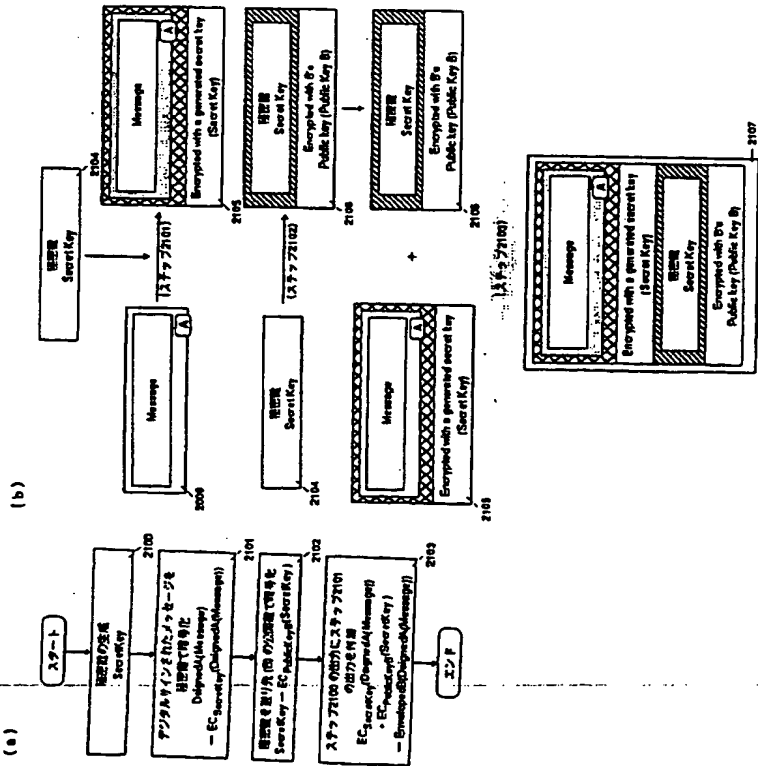


【図19】



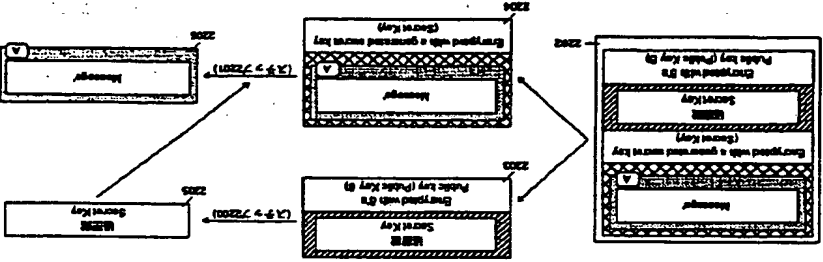
(155)

【図 2 1】



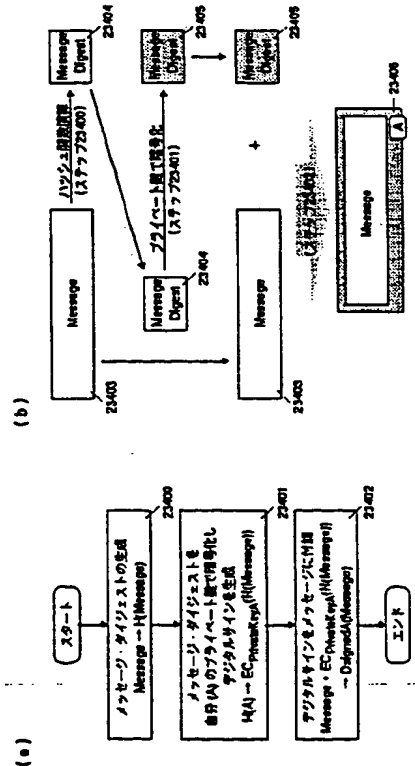
(156)

【図 2 2】



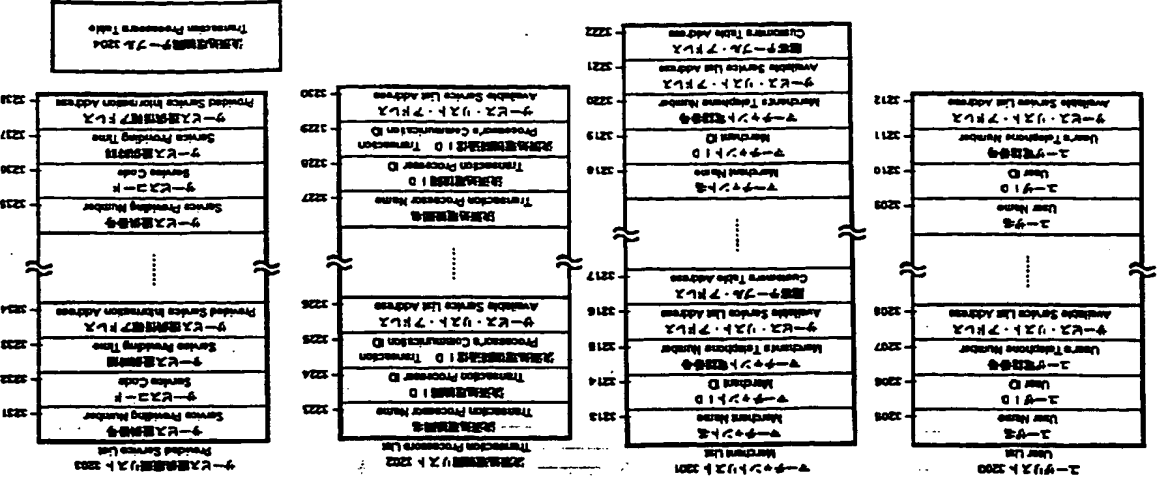
(b)

【図 6 4】

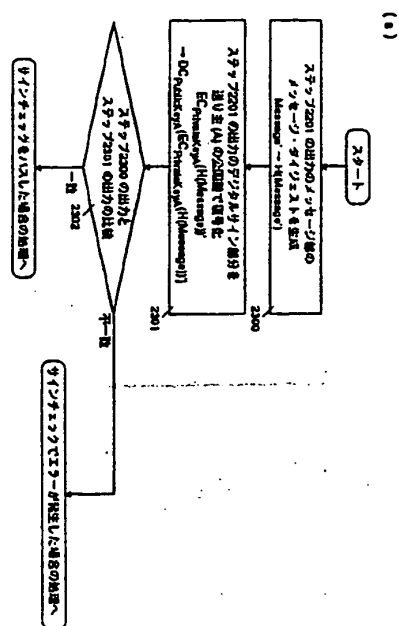


(a)

【図 3 2】

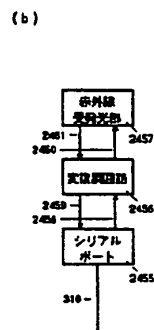


(157)

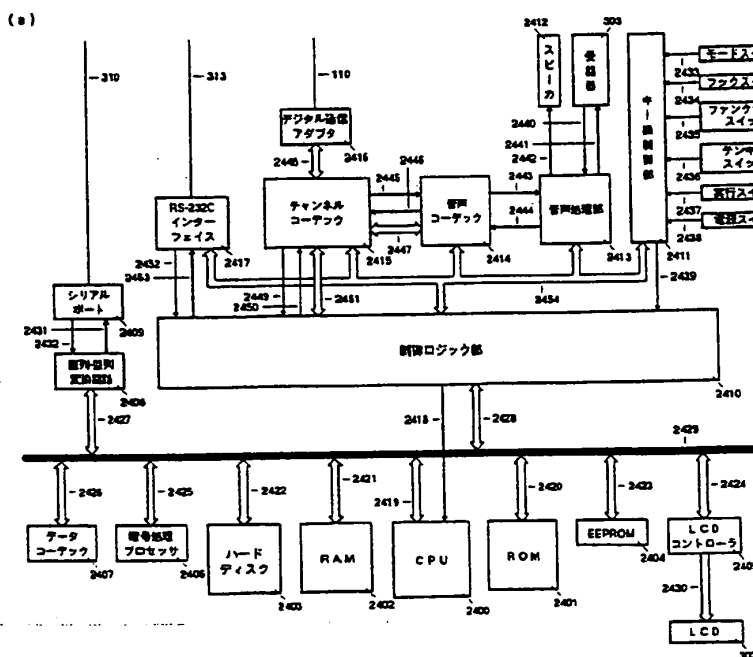


**【圖 23】**

(158)

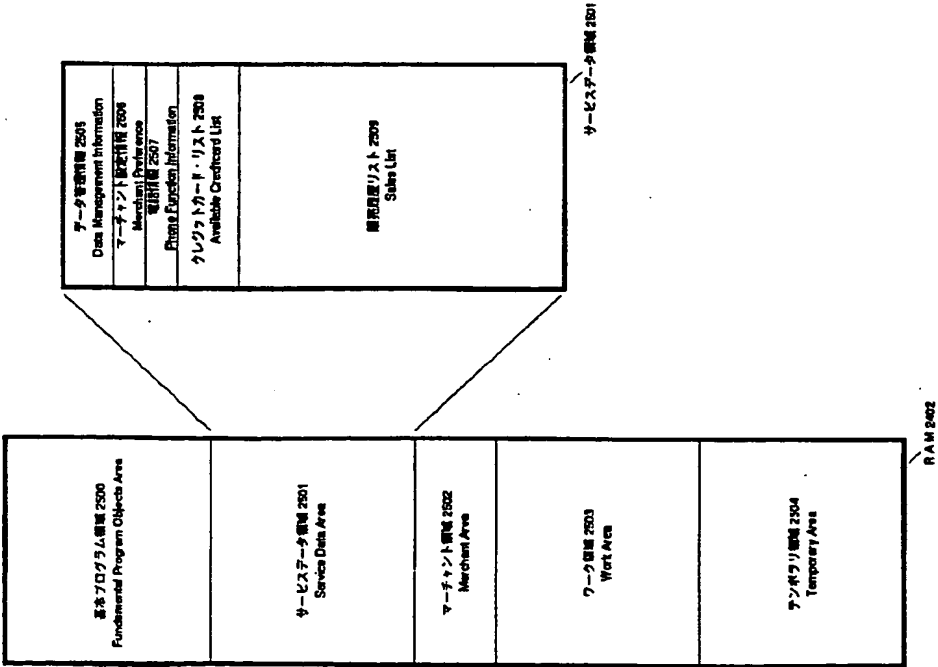


**【例24】**



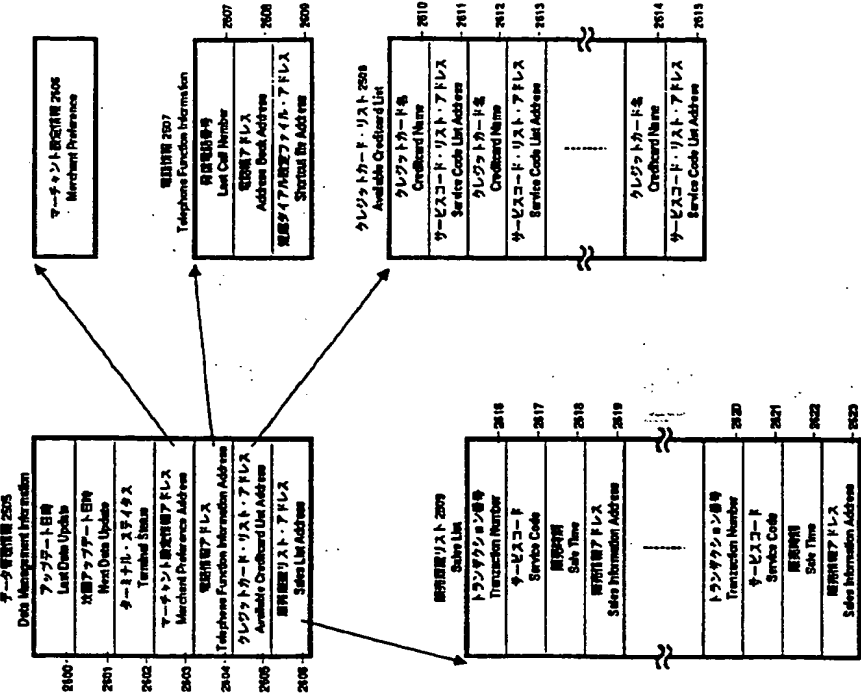
(159)

[図 25]



(160)

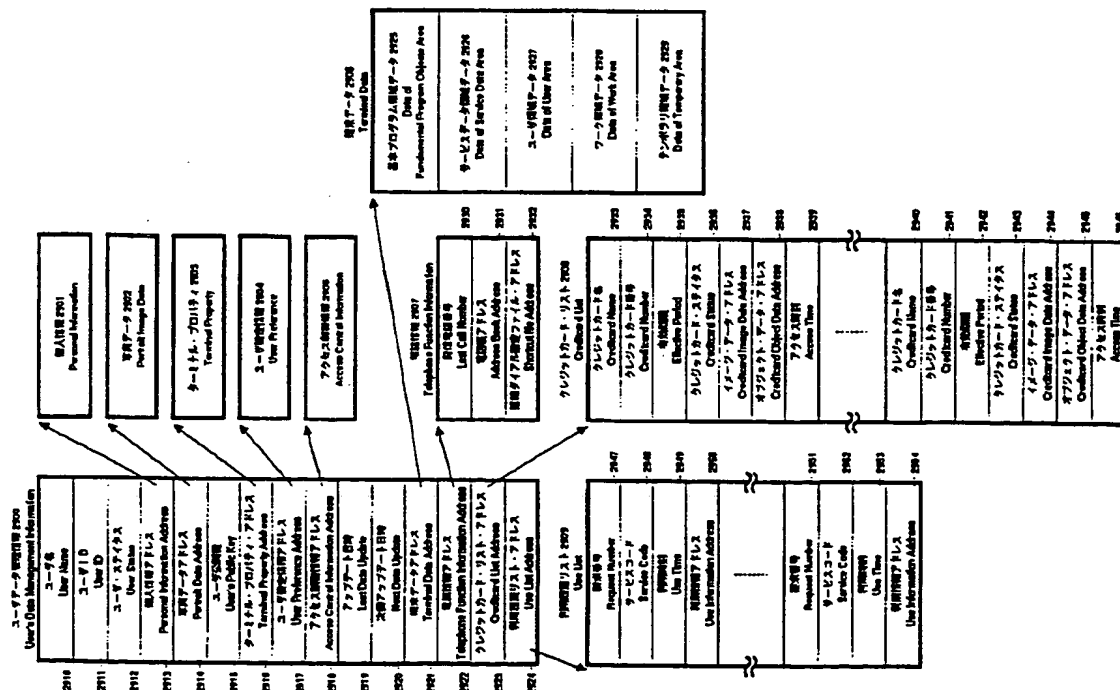
[図 26]





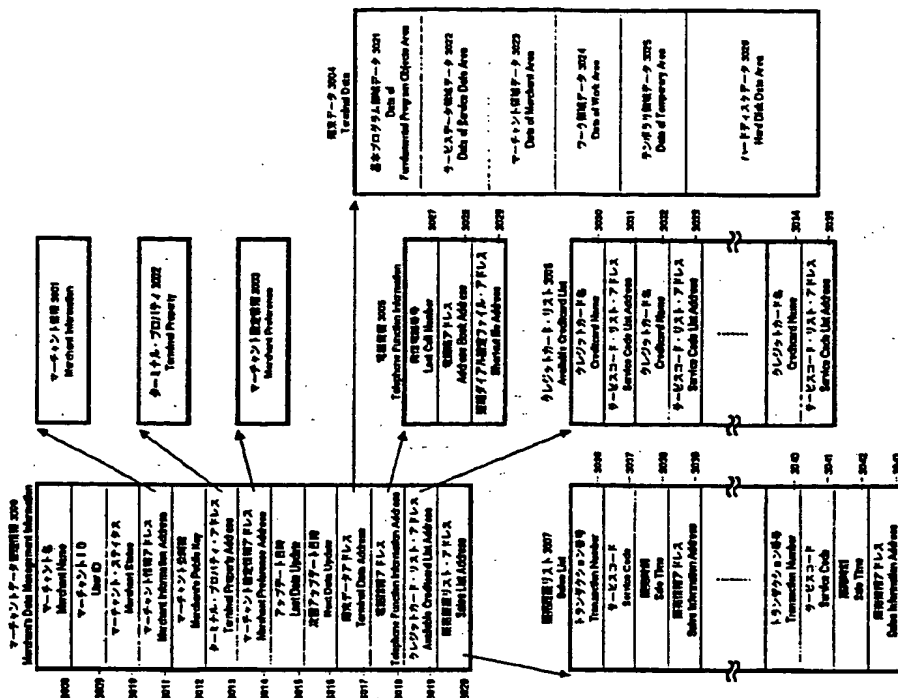
(163)

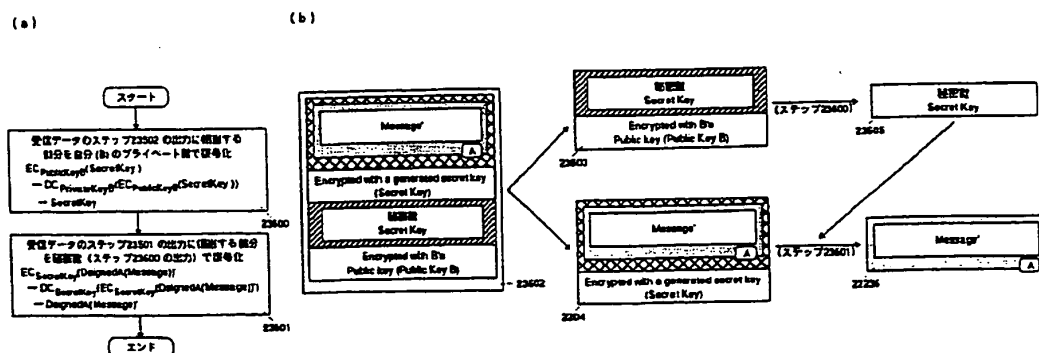
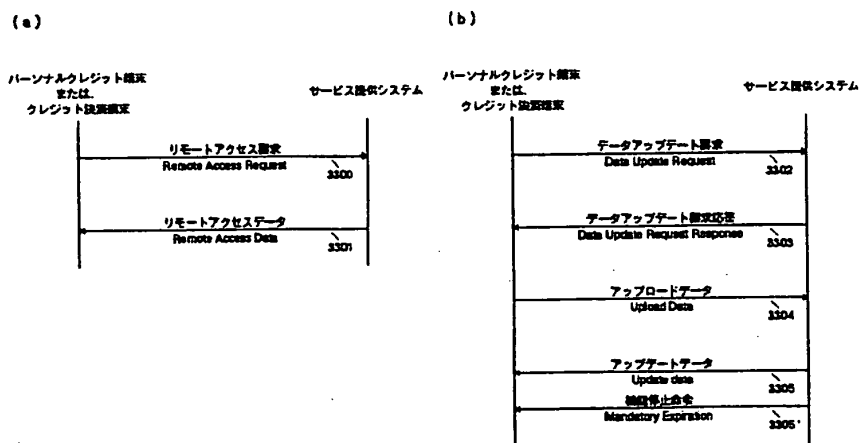
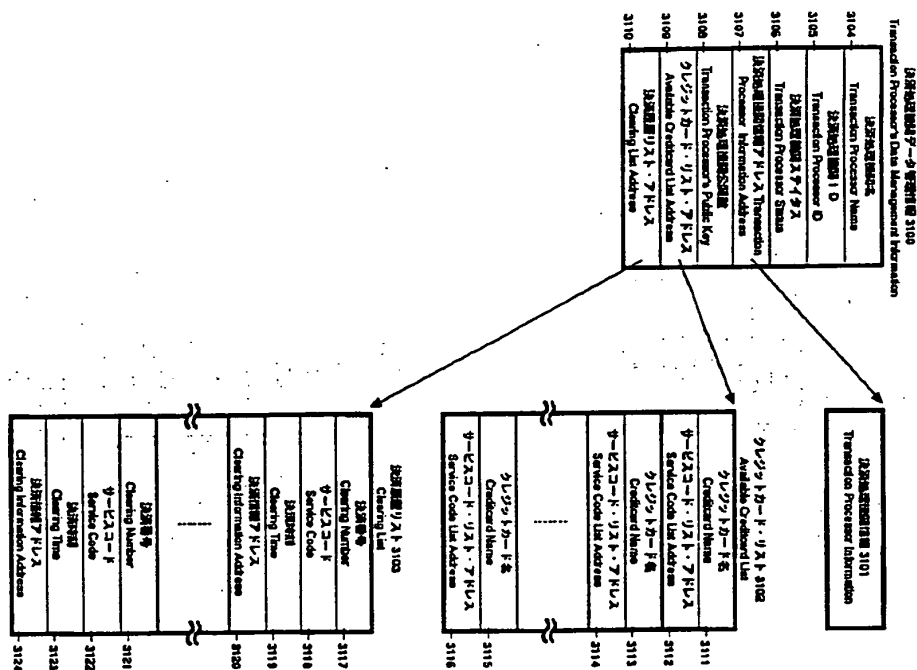
【図29】



(164)

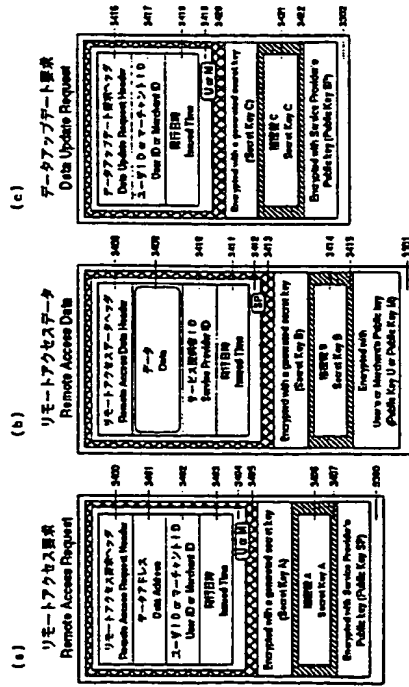
【図30】





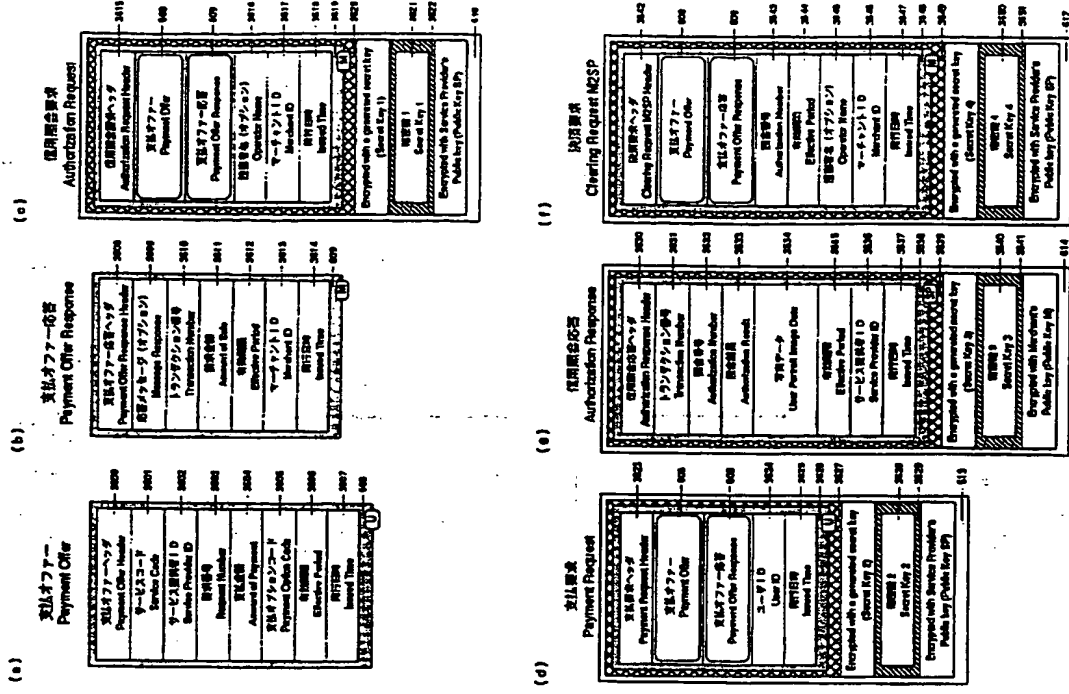
(187)

【図34】



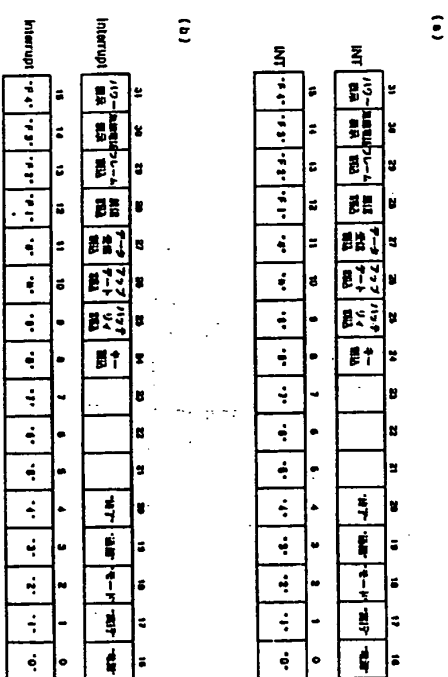
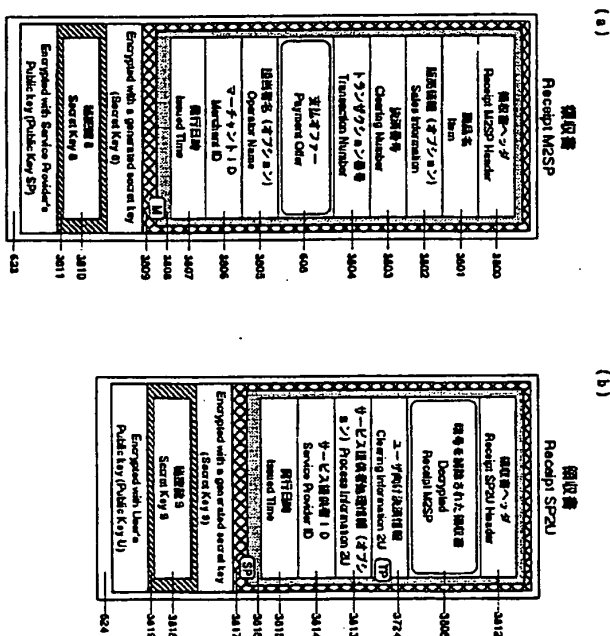
(188)

【図36】



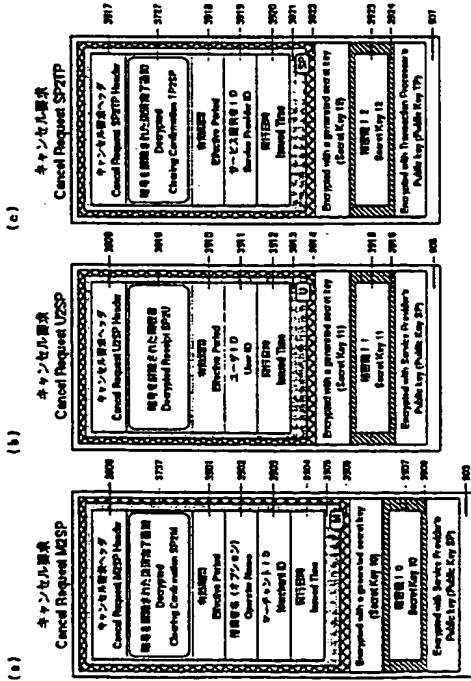


**[ 3 8 ]**



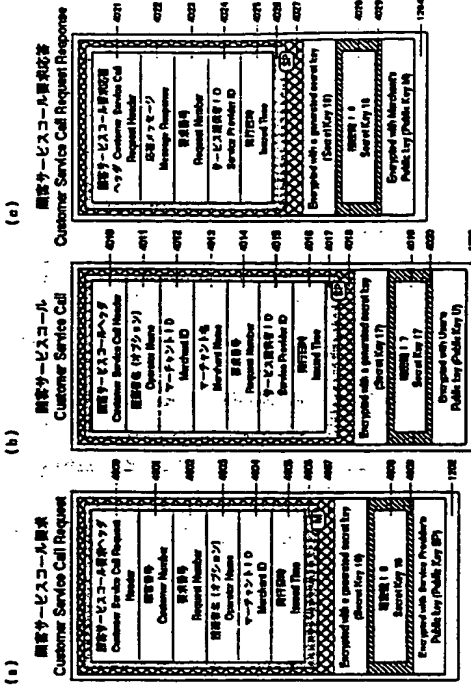
(171)

【図 39】



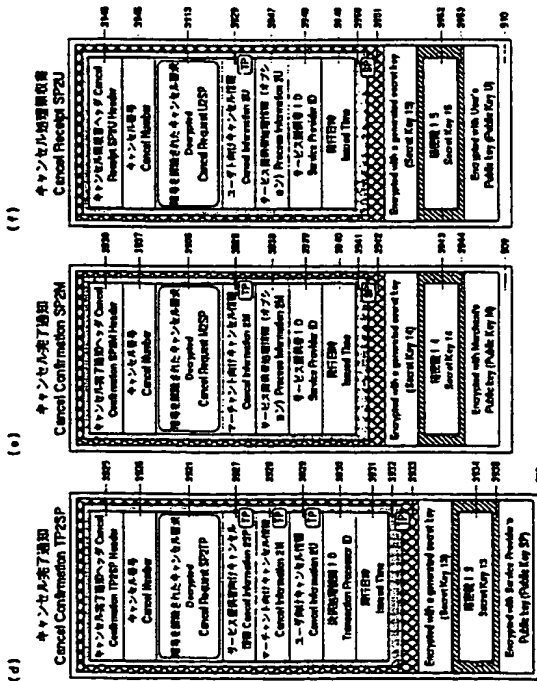
(172)

【図 40】



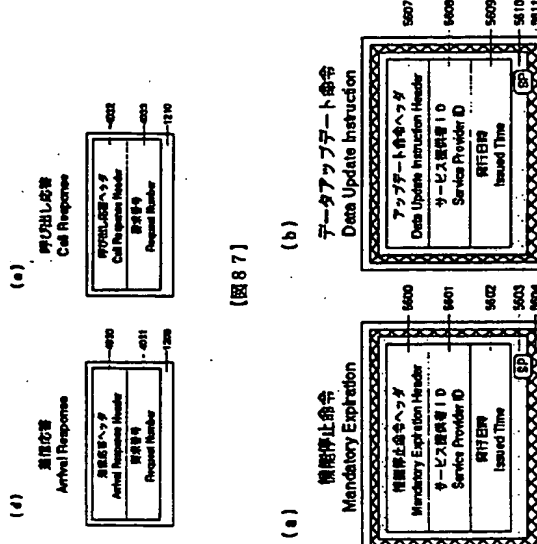
(173)

【図 41】

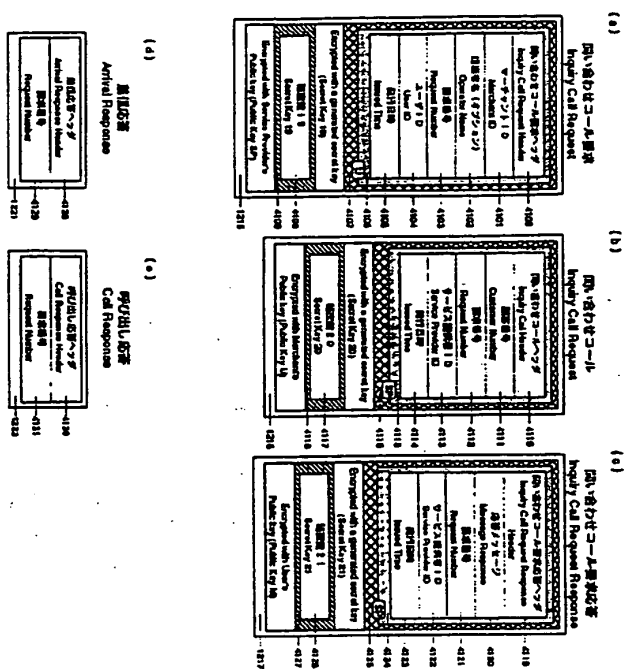


(174)

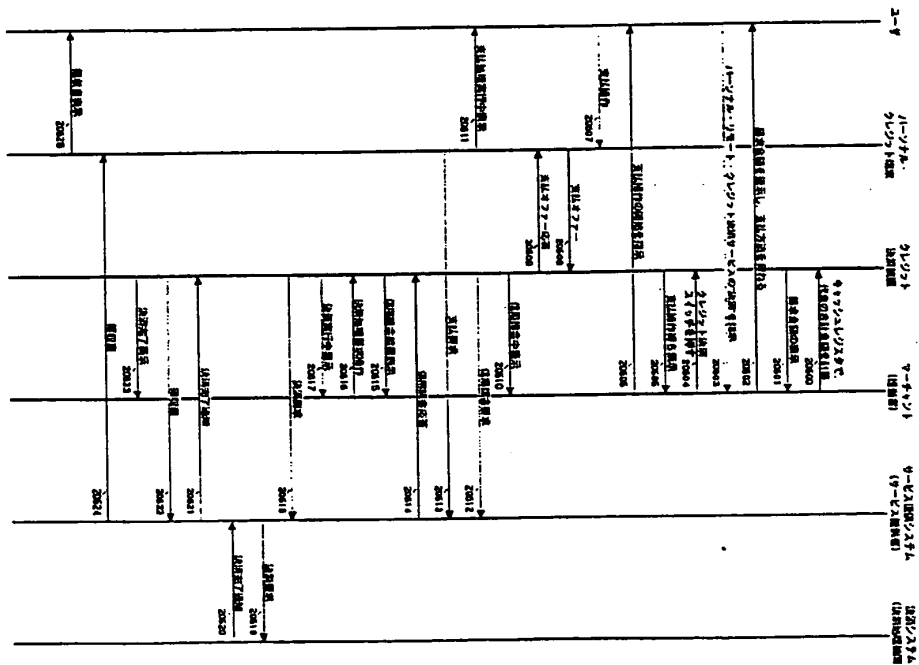
【図 42】



**【圖 4 1】**



**[圖 4.3]**



**【圖44】**

【圖45】

(a) Phone \_\_\_\_\_

Telecommunications Corp.

00000000000000000000
0000
0000
AZLN
BZLN
CZLN

**B Creditcard**

鈴木 太郎  
Taro Suzuki  
5555 6666 7777 8888  
GOOD THRU 12 / 99  
**B CreditCard Corporation**

クレジット会社名  
カード番号  
有効期限  
名前

(c)

A Creditcard

鈴木 太郎  
Taro Suzuki  
1111 2222 3333 4444  
GOOD THRU 12/99  
A CreditCard Corporation

クレジット番号
キヨロギル
利用期限
ヘルプ

[illegible][illegible]

A Creditcard  
 支払  
 ¥20,600  
 1 万円  
 OK 実行  
 キャンセル 終了

(c)

A Creditward

支払処理  
実行中

キャンセル ➡ (終了)

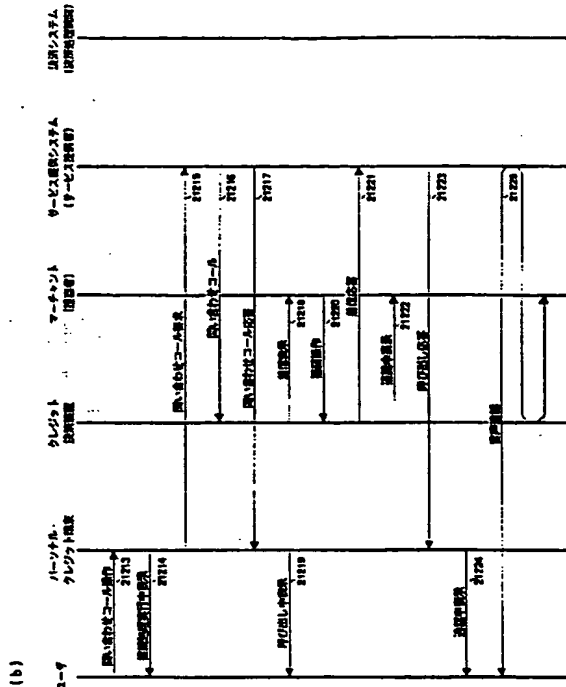
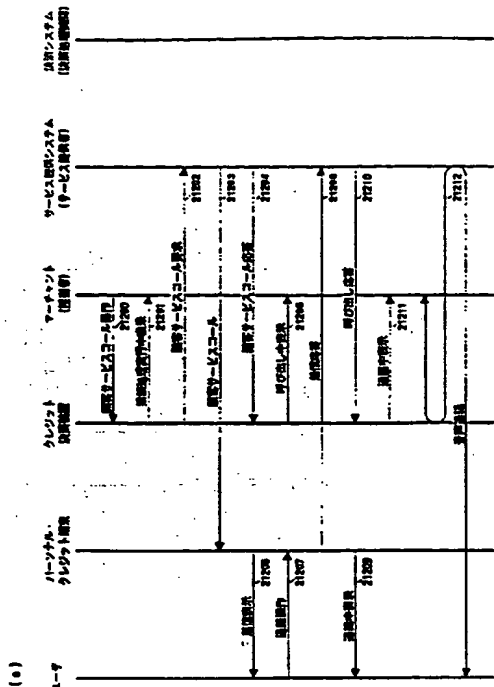
A Credited		2001.09.07 19:24:31
領收書		
用途	附屬	金額
禮品A	I	2,000
禮品B	I	7,000
禮品C	I	10,000
小計		190,000
收款		900
合計		190,900
支払 A Credited 領收		
○×△領收 附屬：佐藤		
×××××-△△△△△		

(1)

A Creditcard  
¥30,000  
と入力されましたが、  
支払いは、  
¥20,000  
(現金決済)  
でよろしいですか。

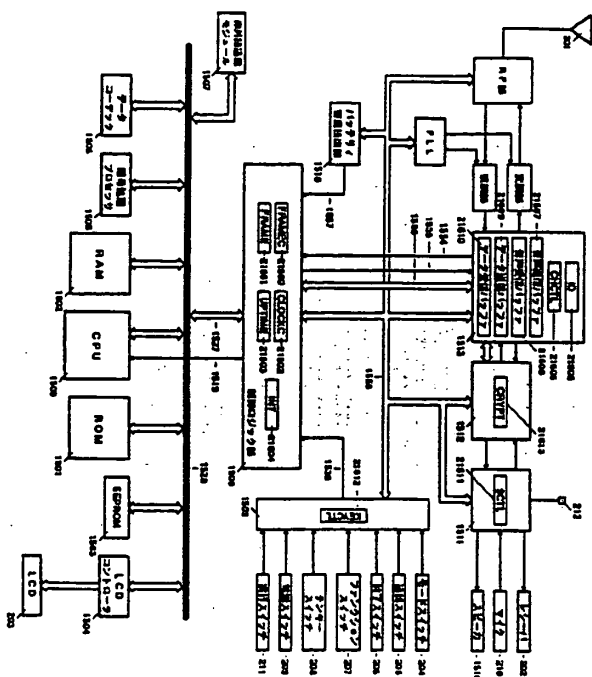
OK ➡ 実行

キャンセル ➡ 終了

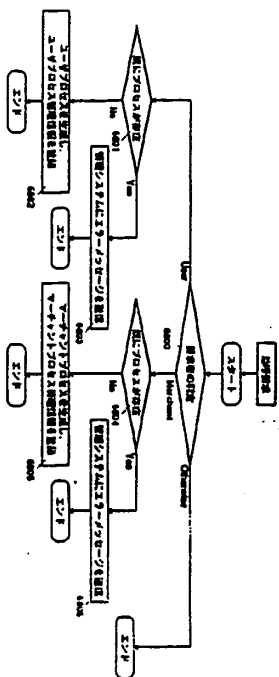


(177)

【図46】

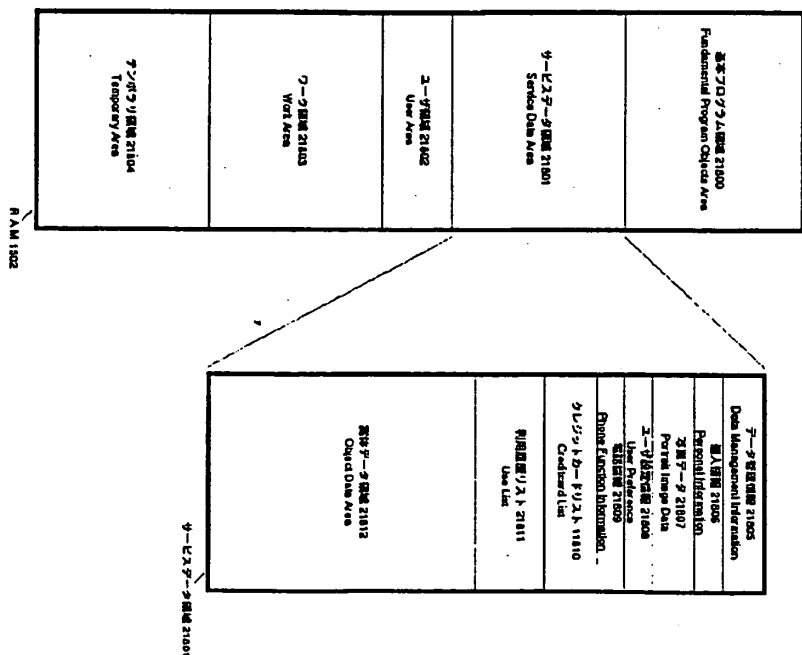


【図49】

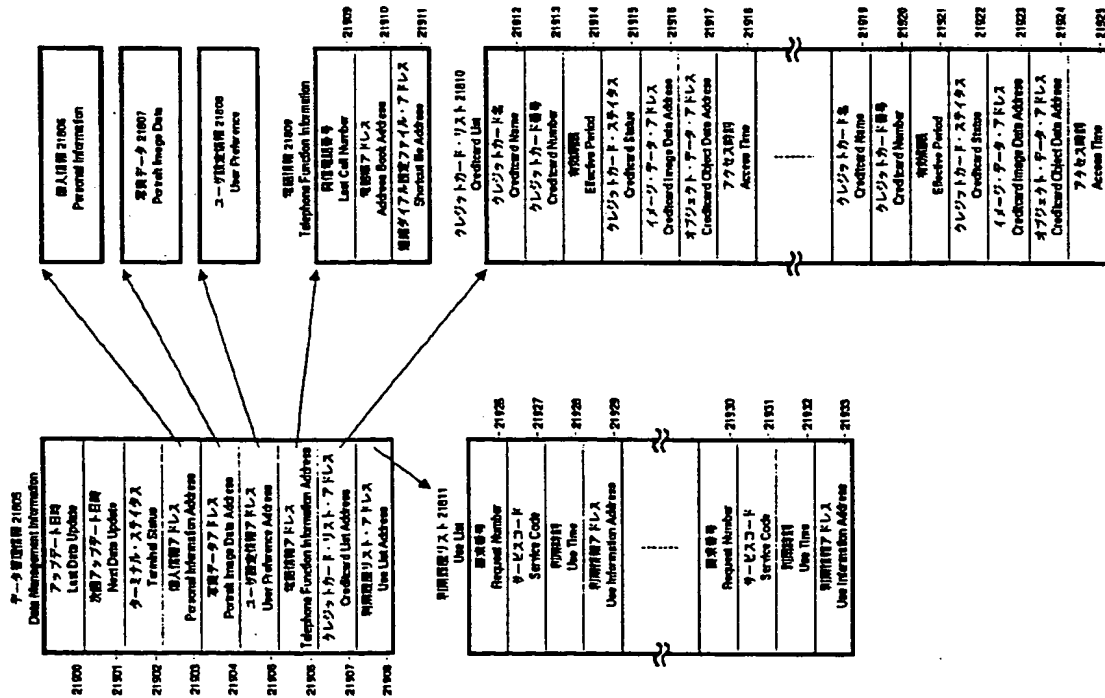


(178)

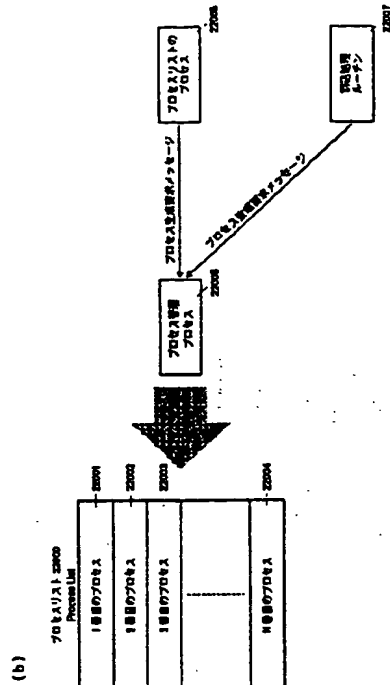
【図48】



【圖 49】

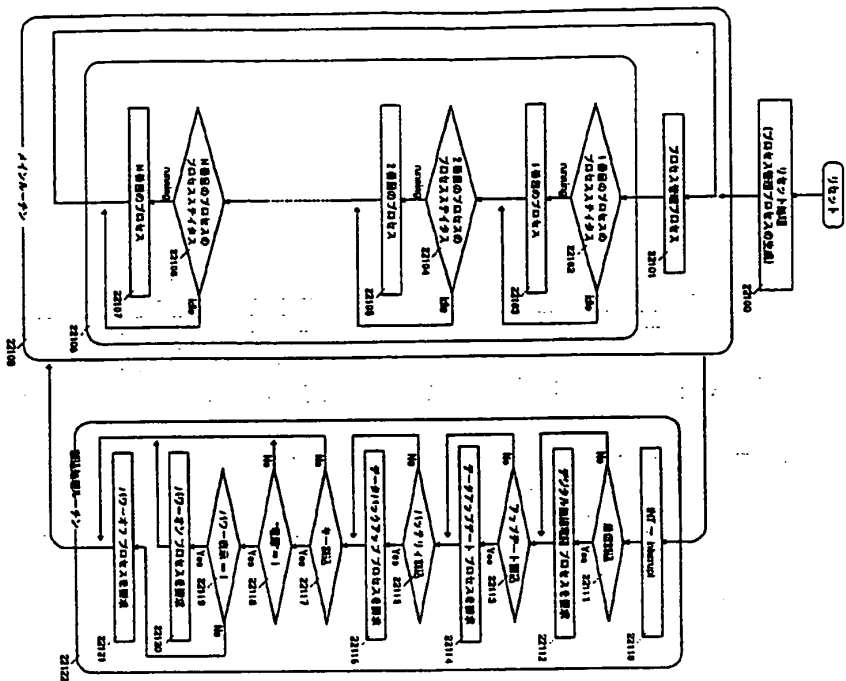


**【圖 50】**

[illegible]

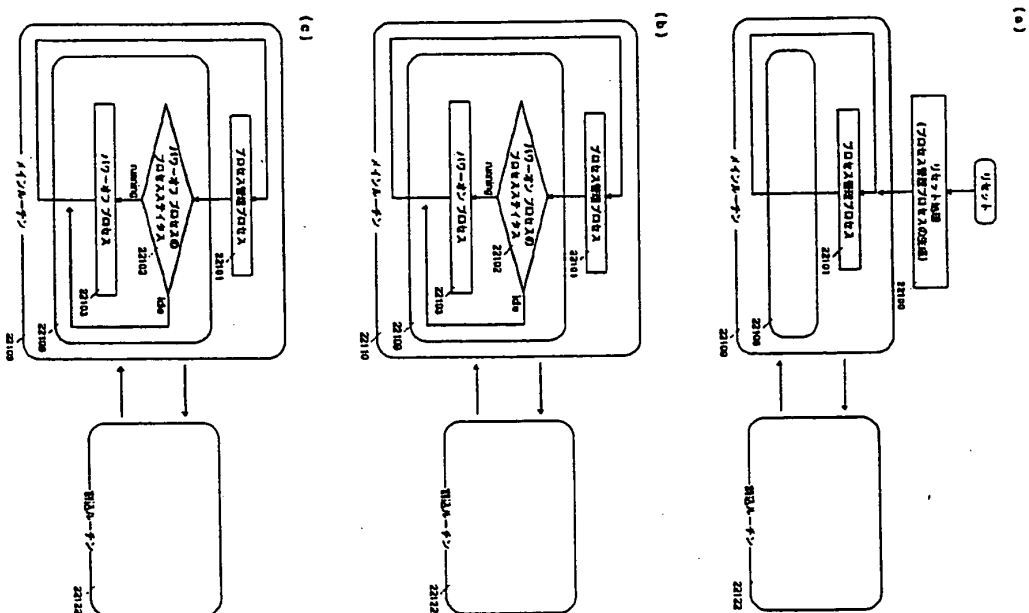
(181)

【図5.1】



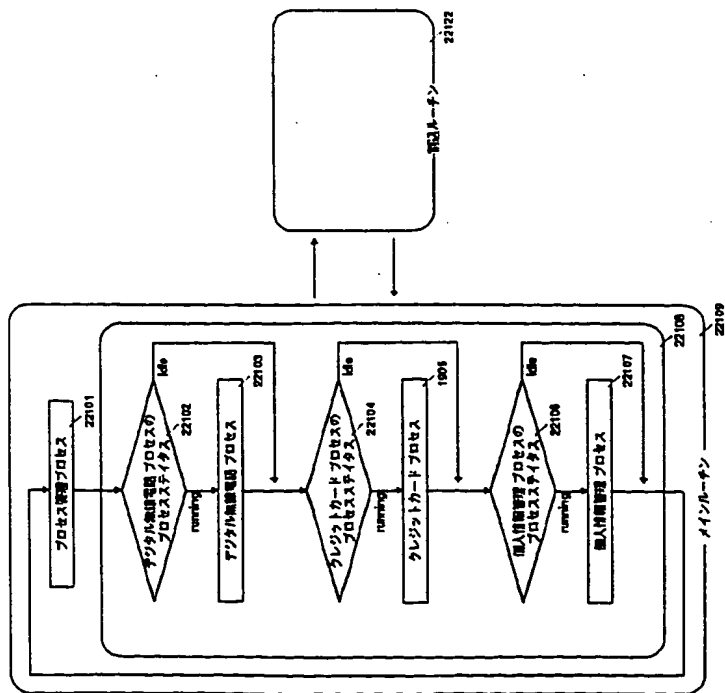
(182)

【図5.2】



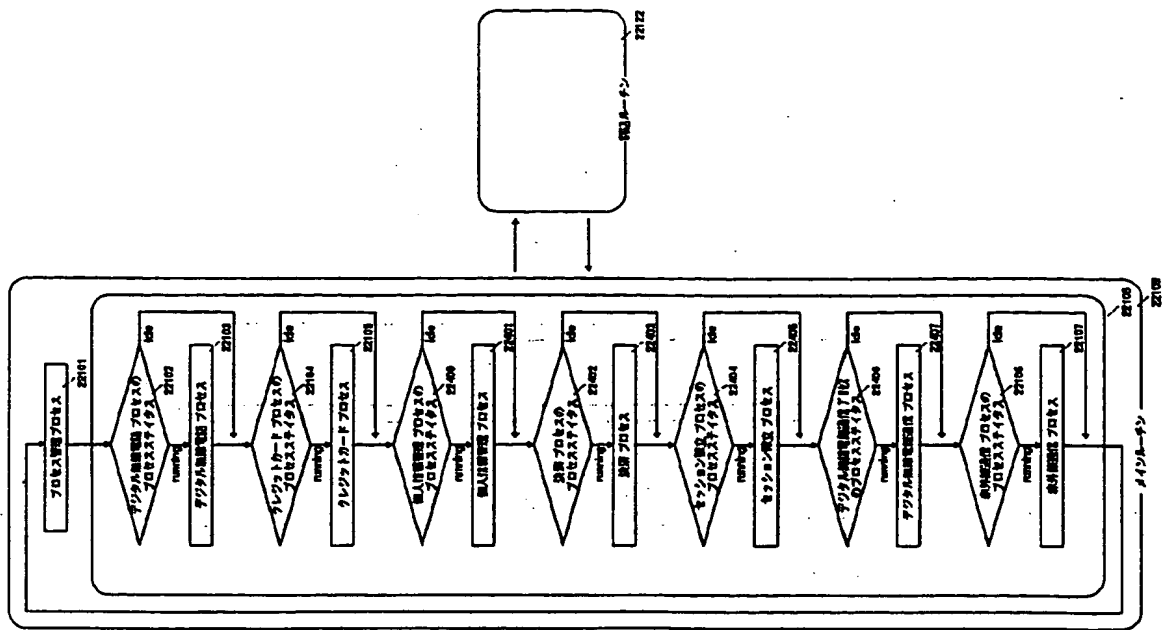
(183)

**【圖 53】**



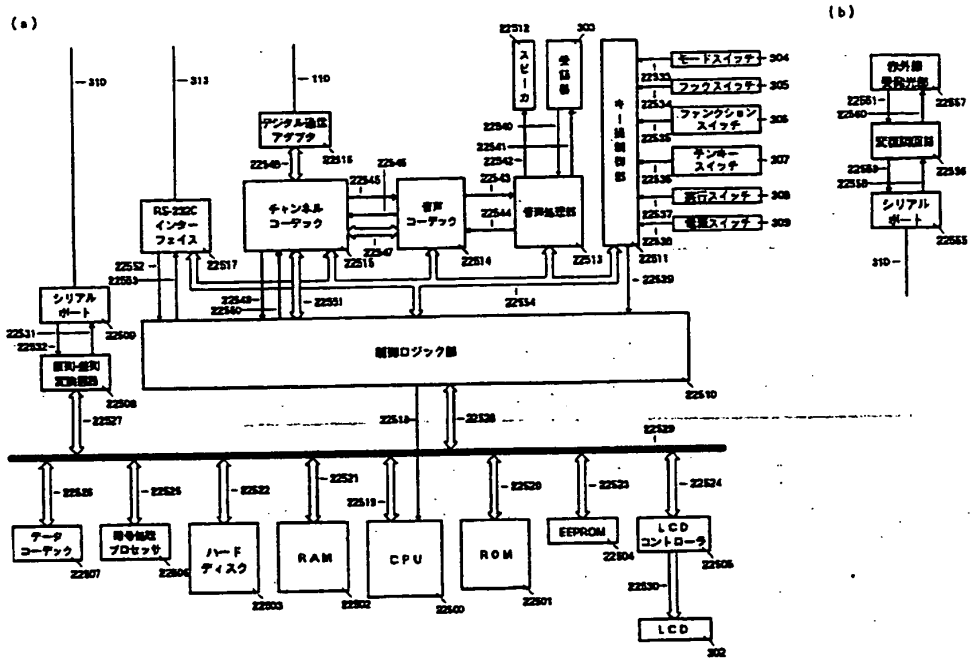
(184)

**{圖54}**

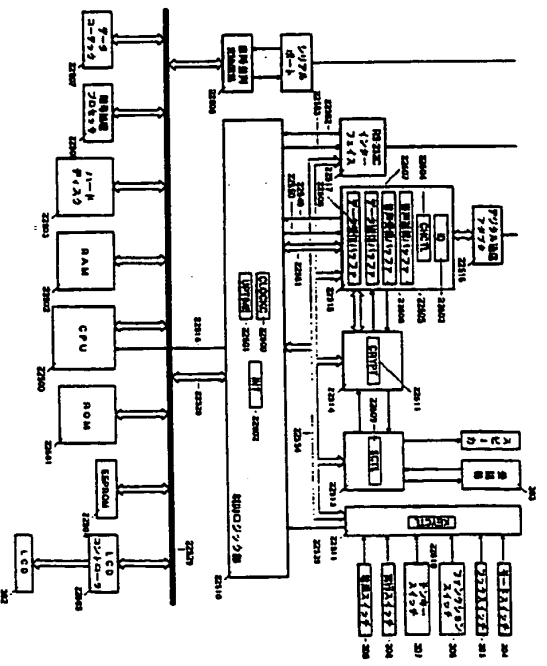




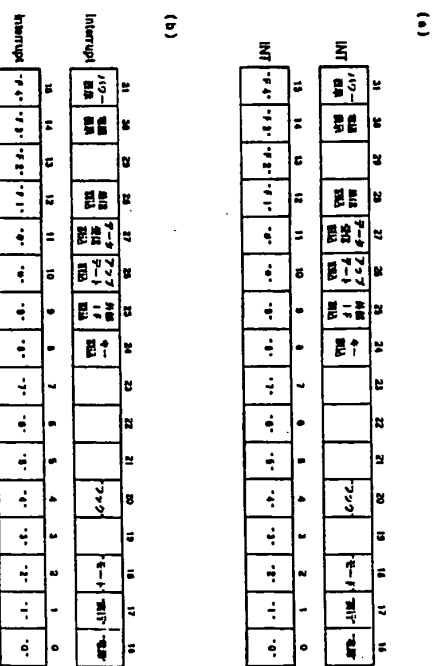
【図55】



【図56】

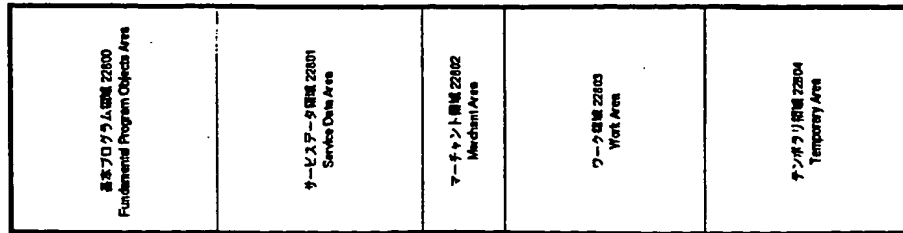


【図57】



(187)

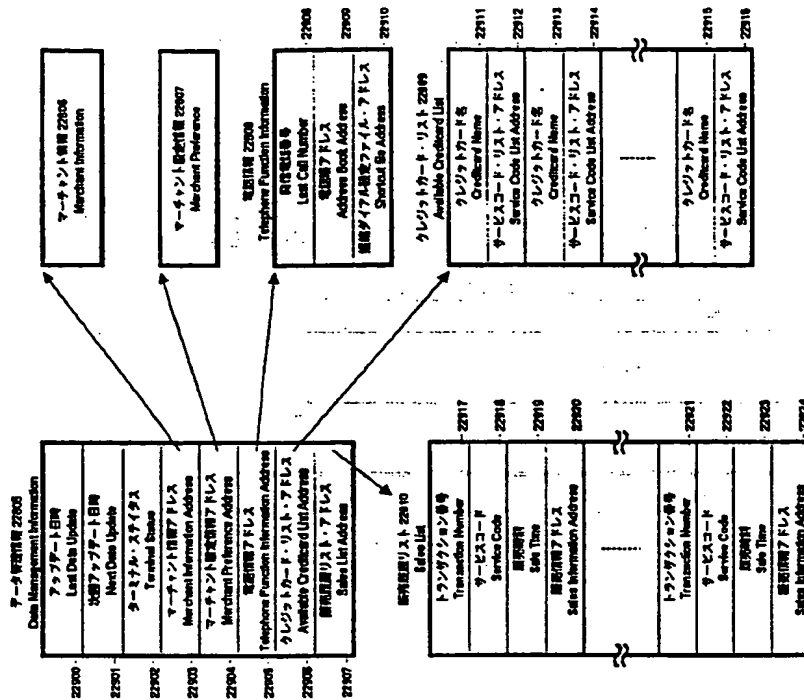
(図58)



RAM 22802

(188)

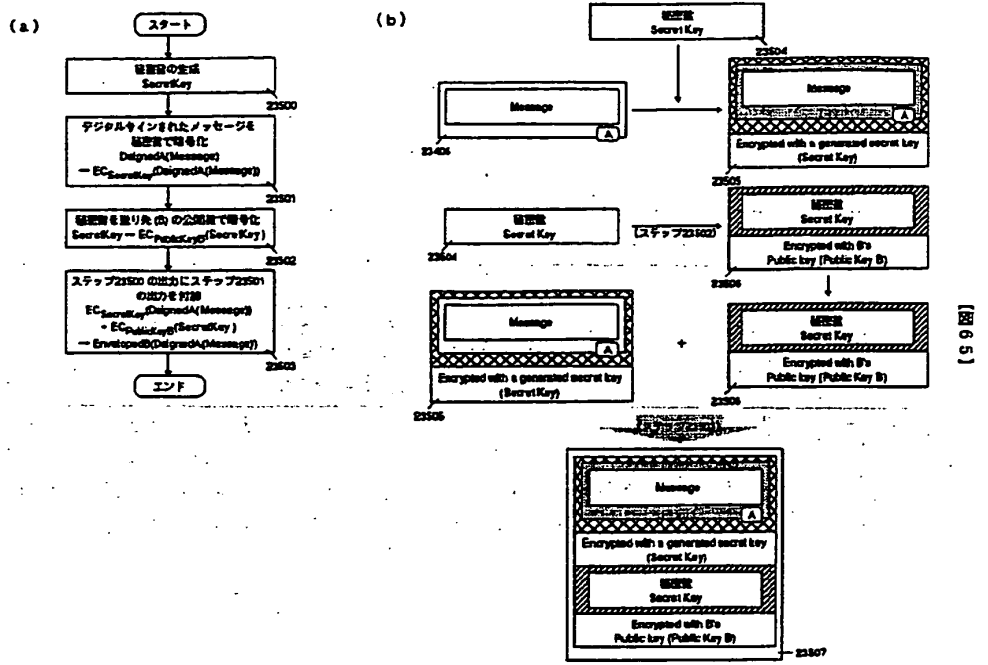
(図59)



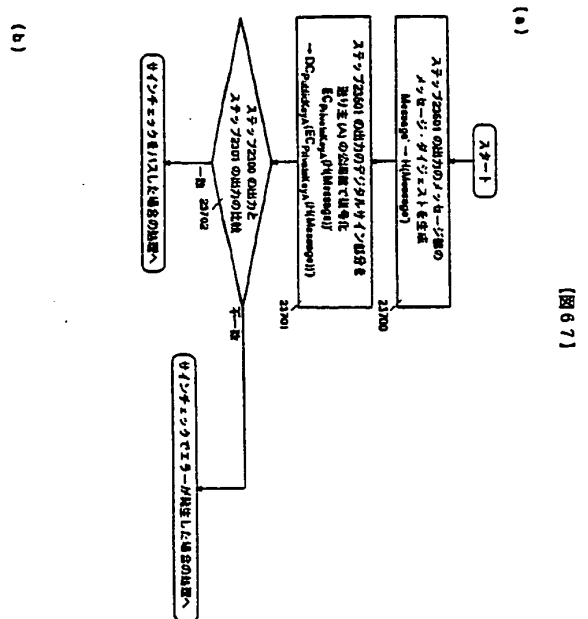




(193)



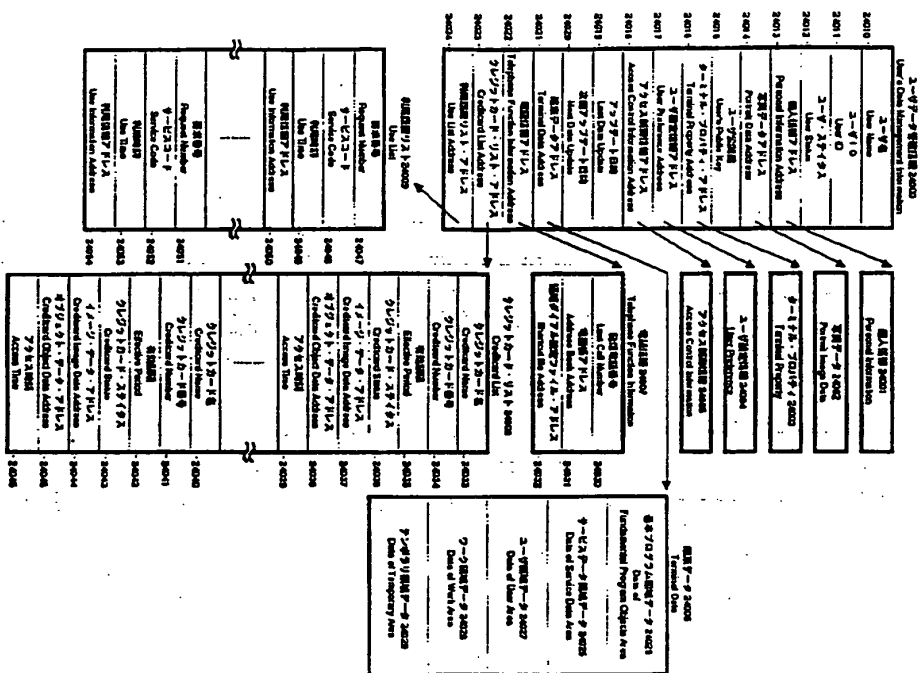
(194)





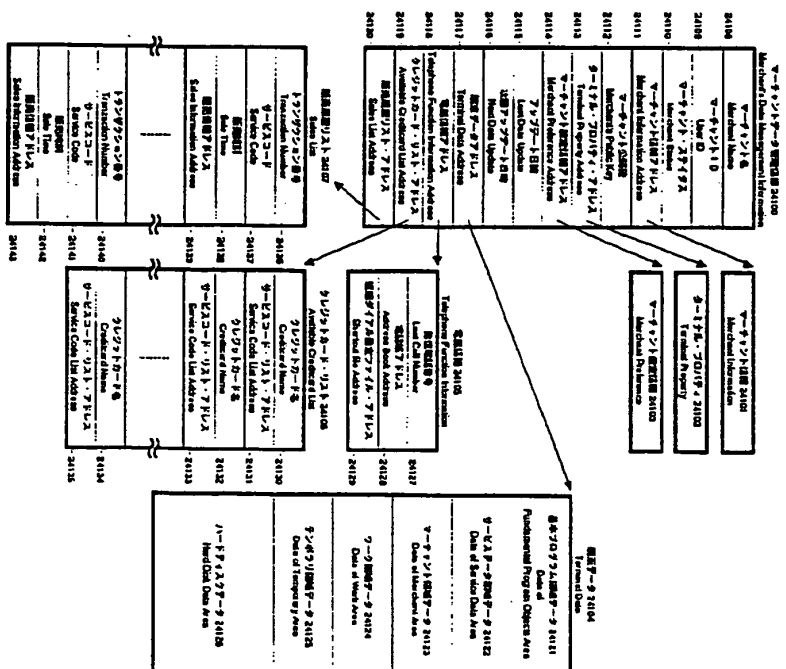
(197)

【図7.1】



(198)

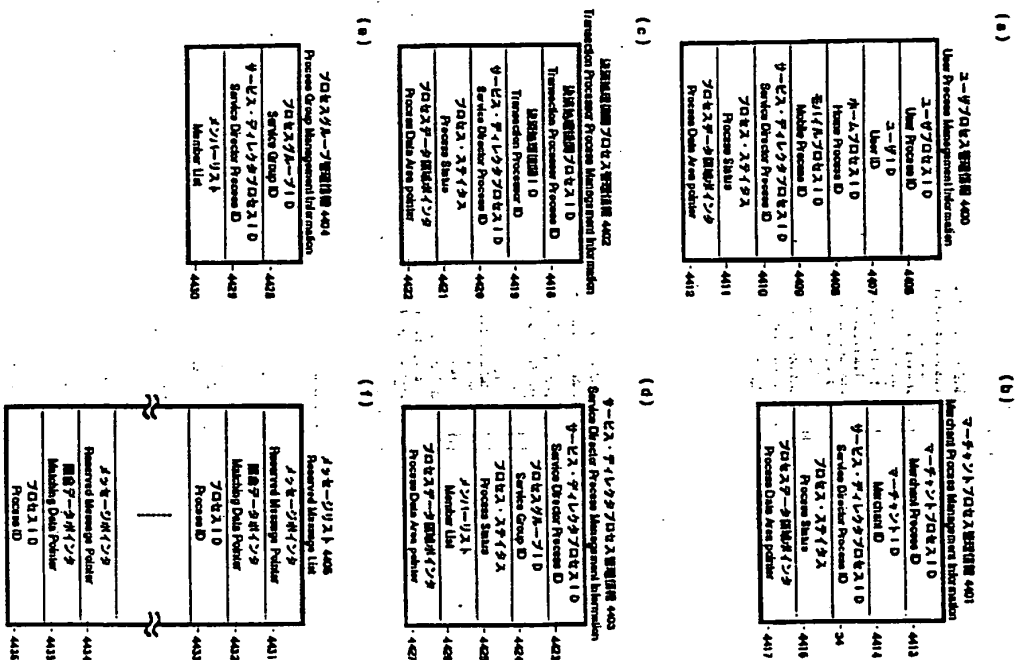
【図7.2】



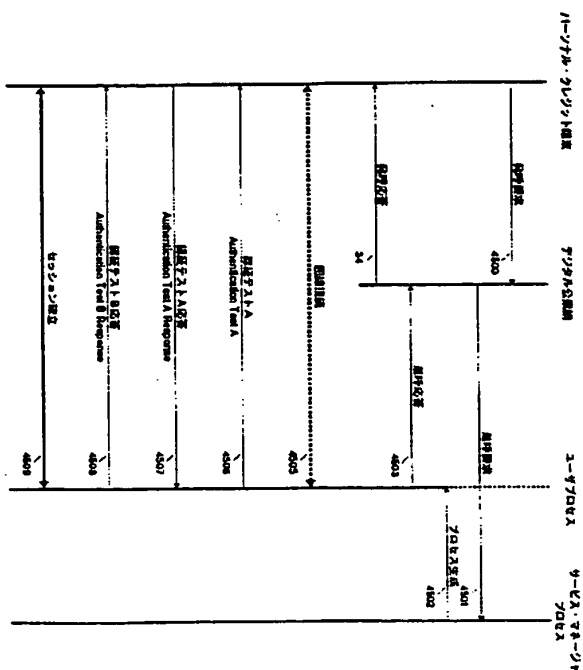




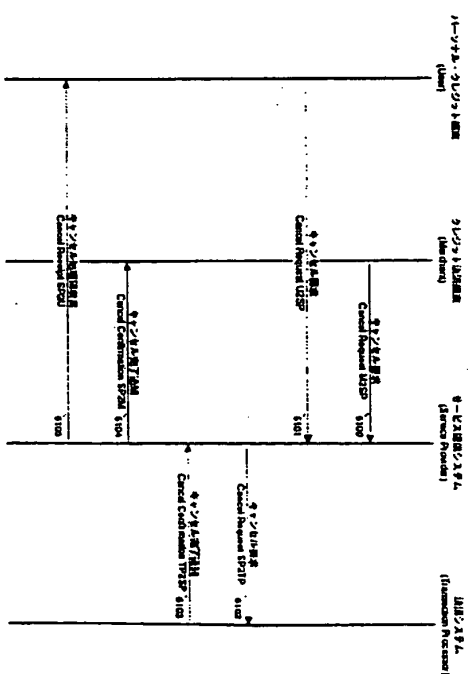
【例 75】



**【圖76】**

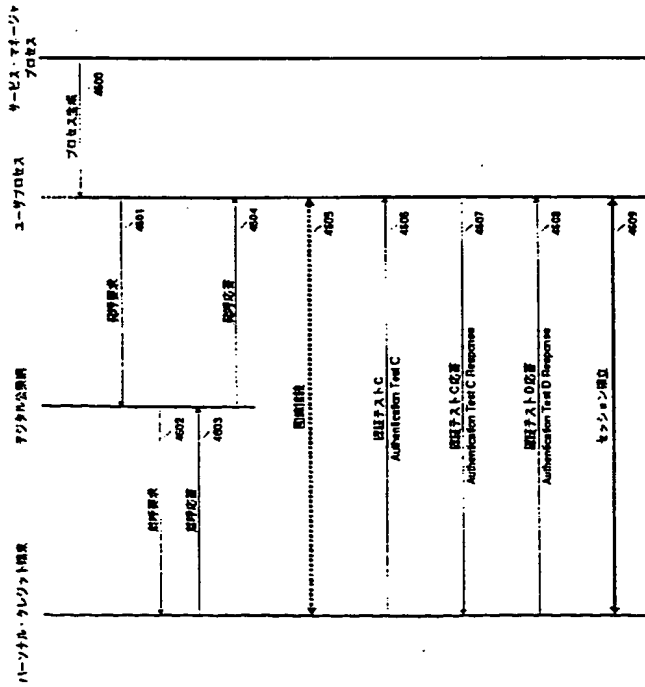


【例 9 2】



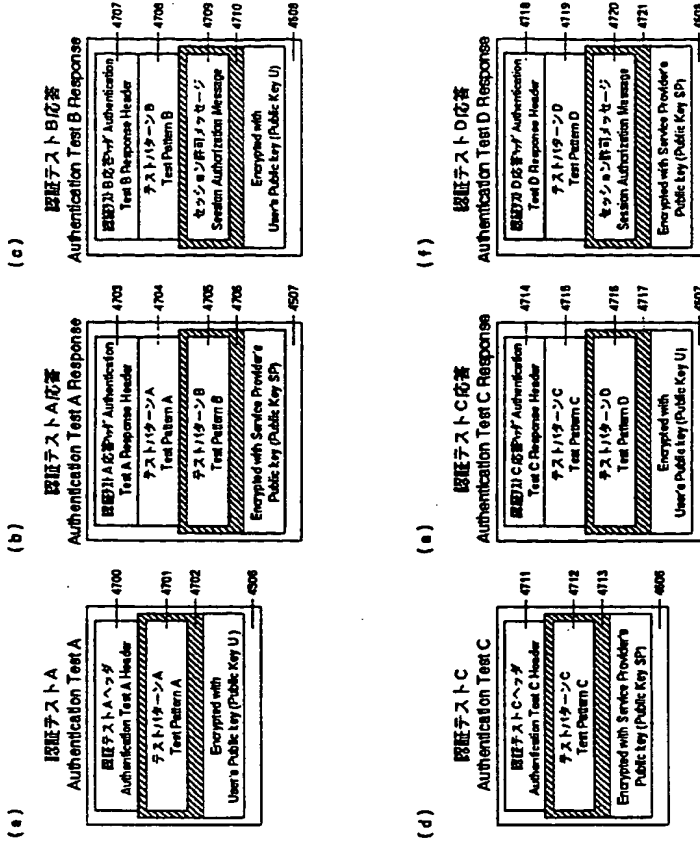
(203)

【図 7 7】

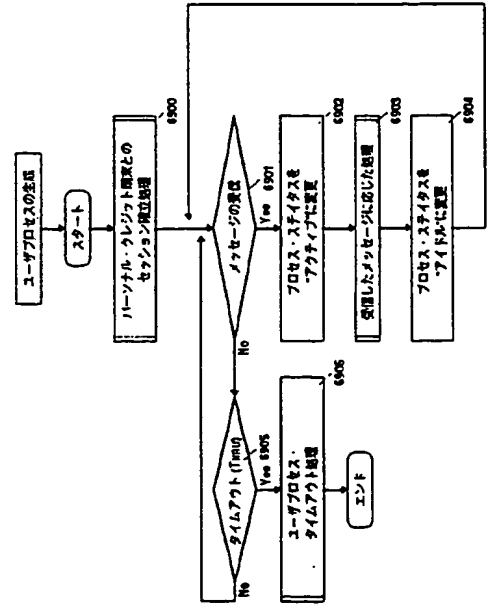


(204)

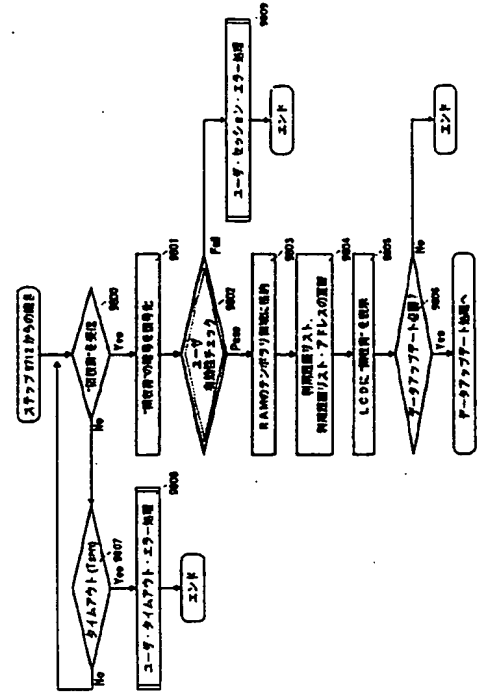
【図 7 8】

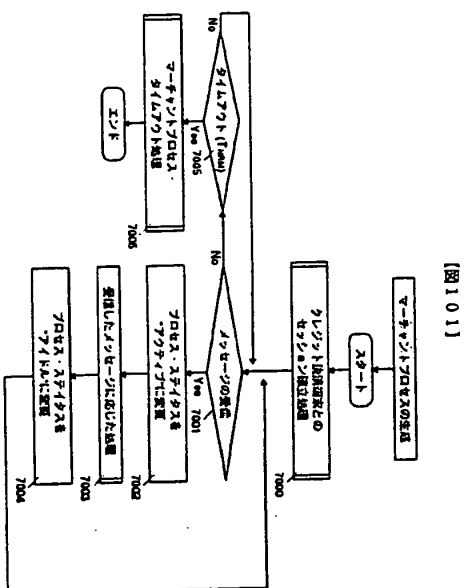
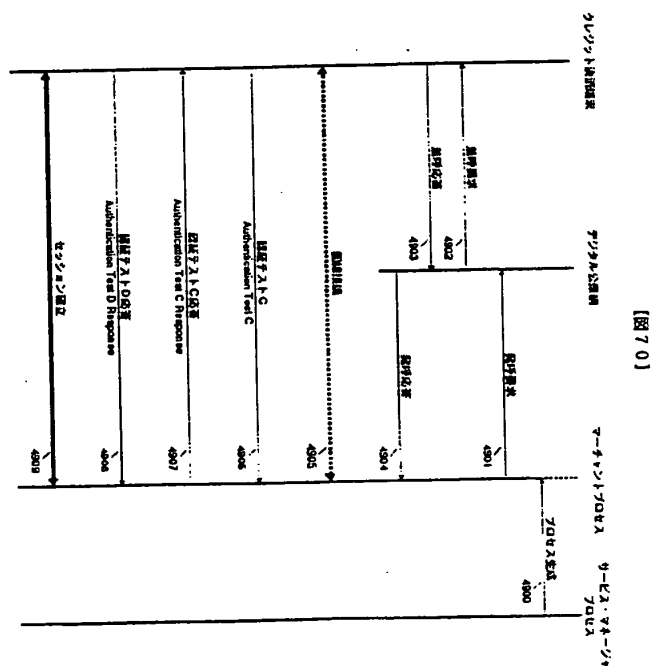
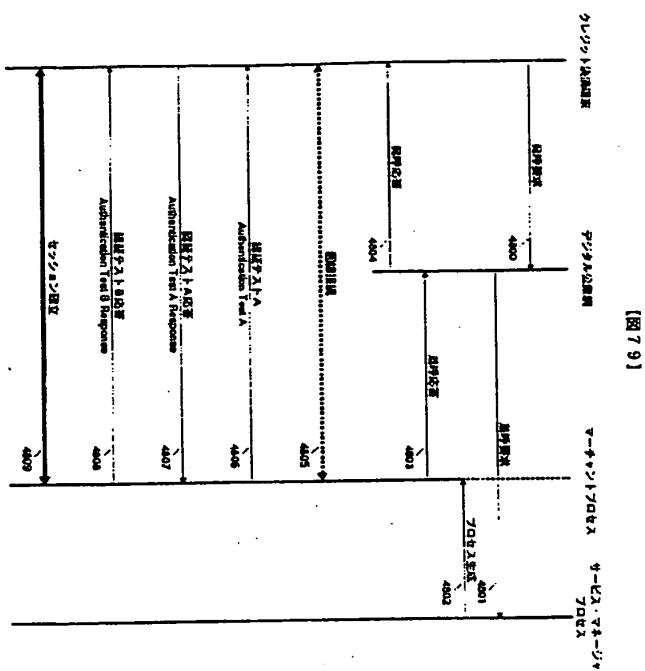


【図 1 0 0】



【図 1 2 9】

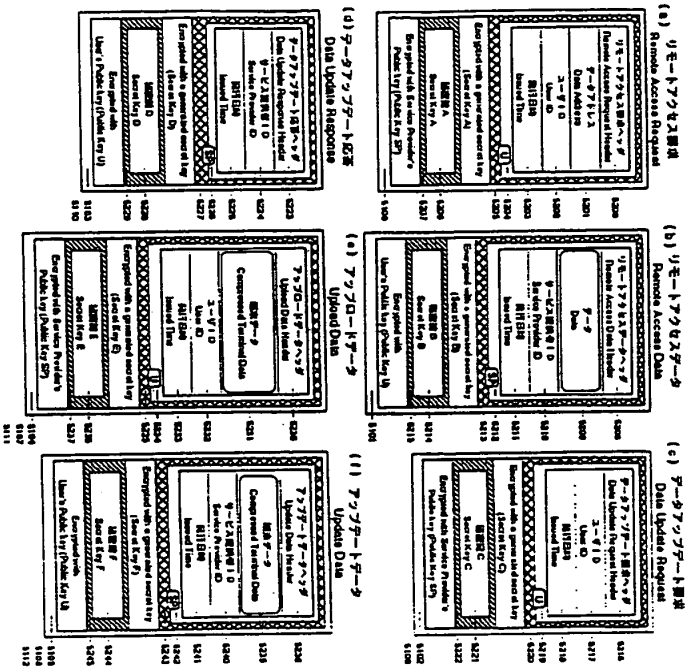






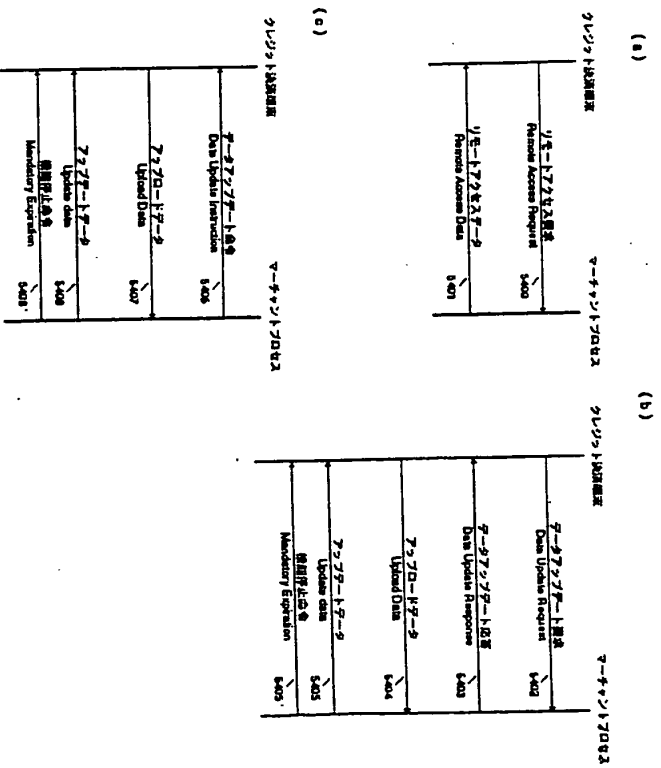
(209)

[図 8.3]



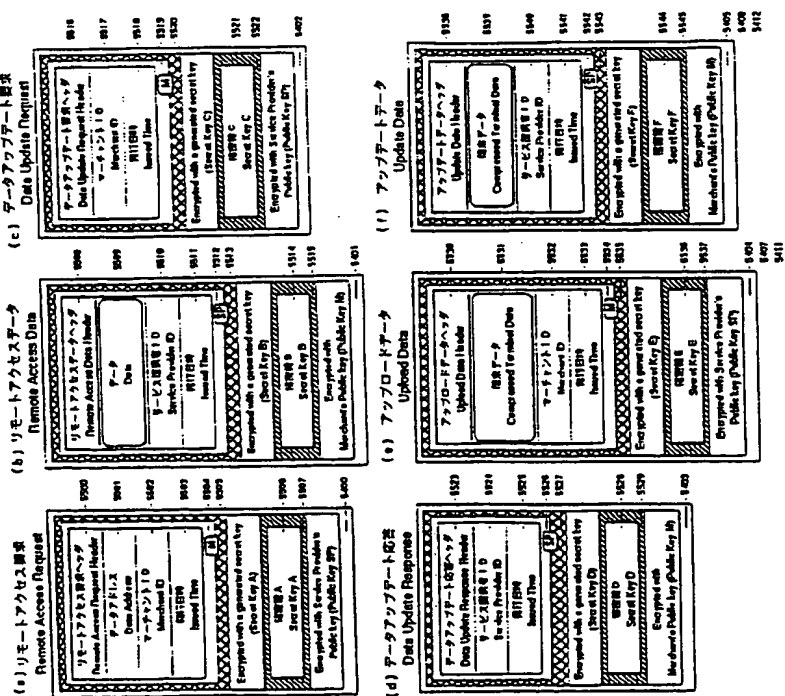
(210)

[図 8.5]



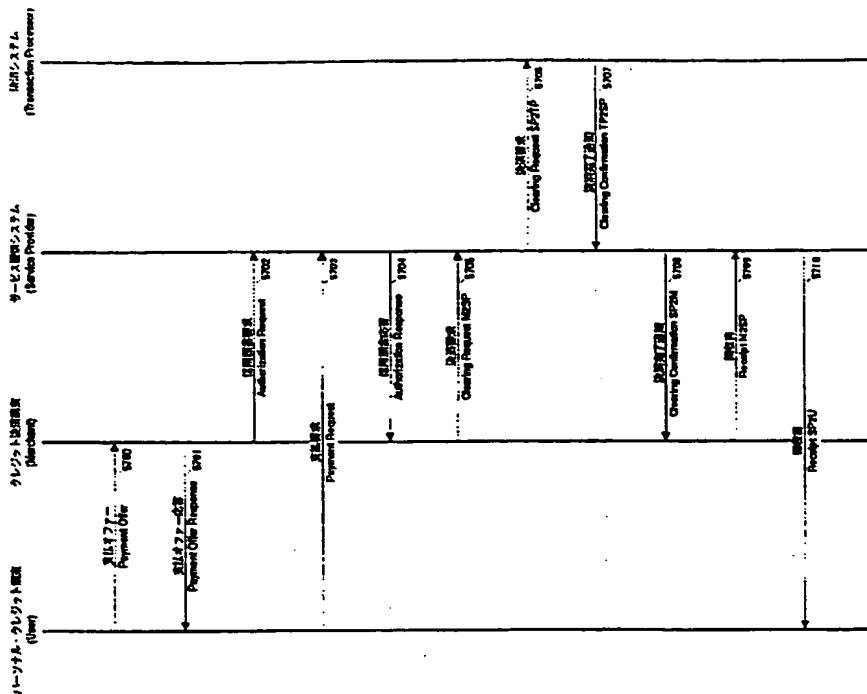
(211)

【図86】



(212)

【図88】



**[06圖]**

[illegible]

**自由新聞會館**  
**Advertisement Request**

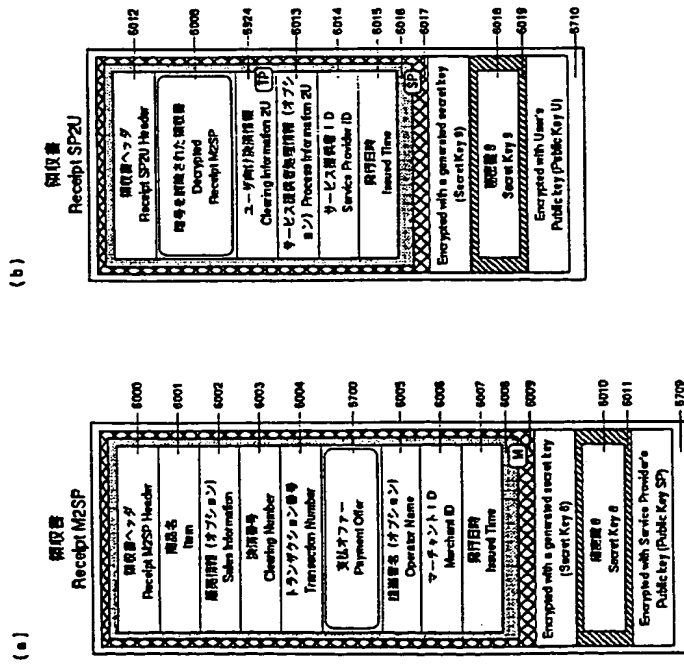
申込者 申込者名 申込者住所 申込者電話番号	掲載希望の新聞 掲載希望の曜日 掲載希望の期間 掲載希望の料金 掲載希望の備考
---------------------------------	---

自由新聞會館 受付

[illegible]

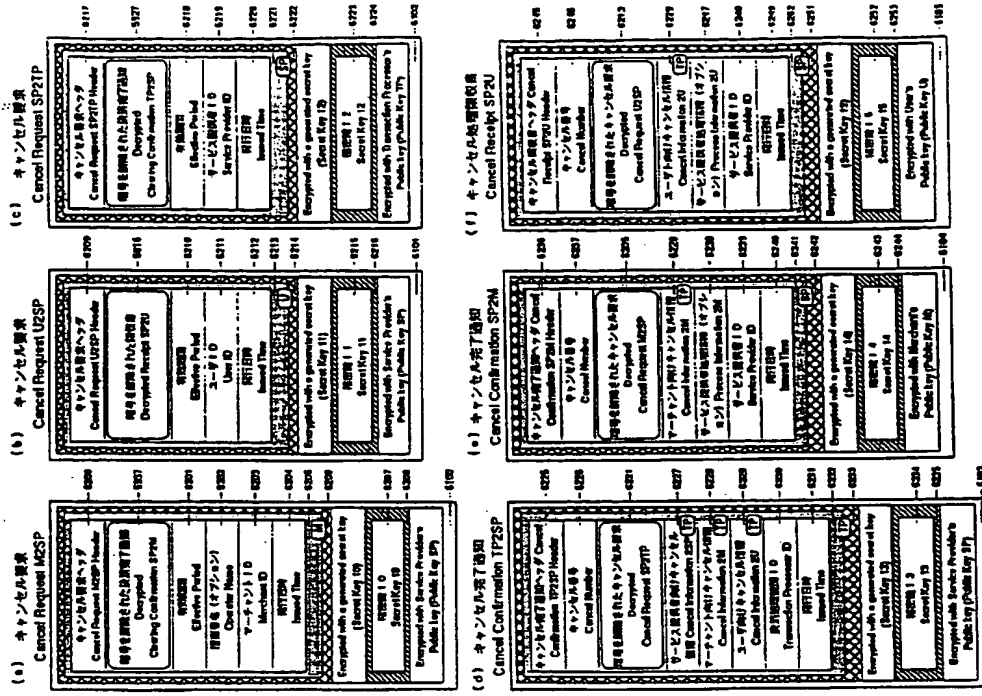
(215)

[図91]

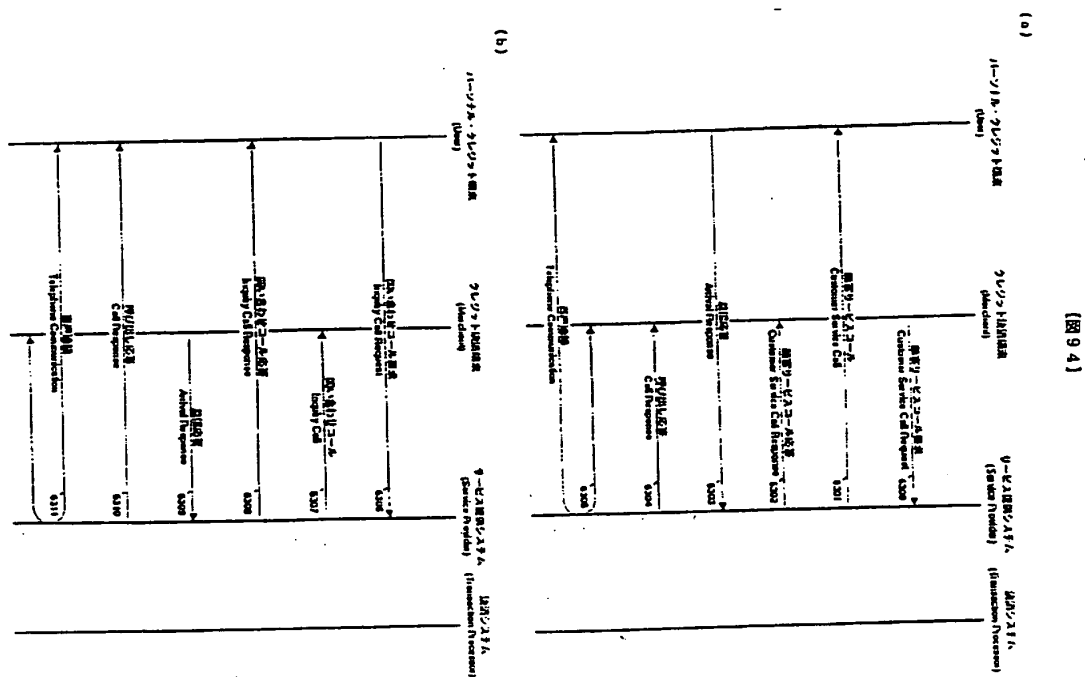


(216)

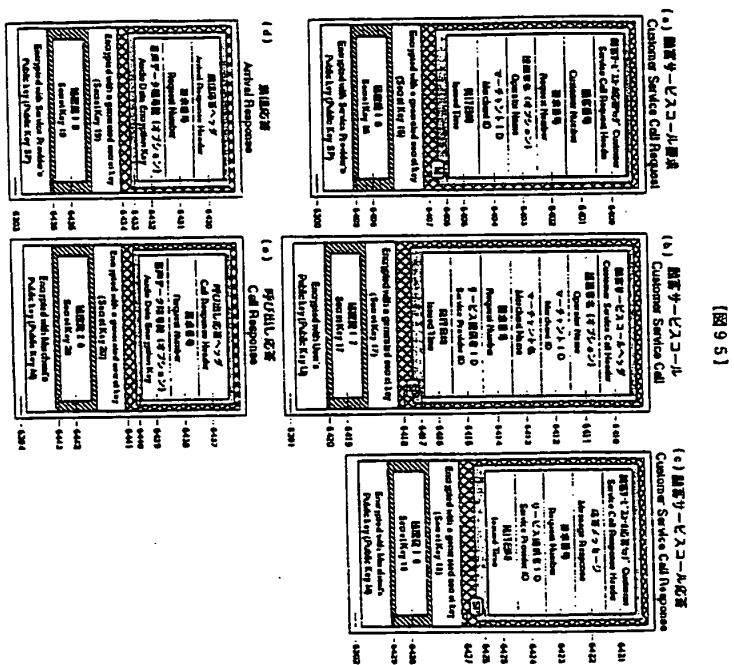
[図93]





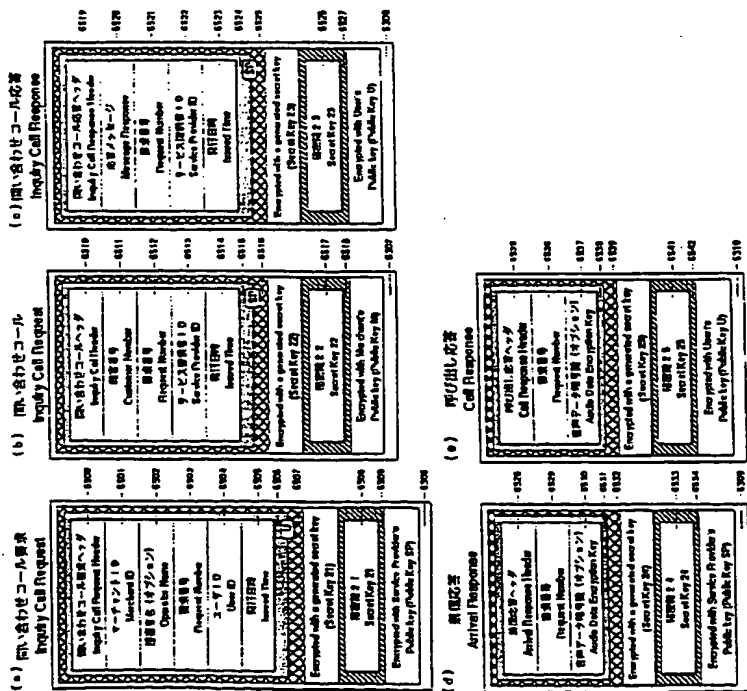


**【例 9 4】**

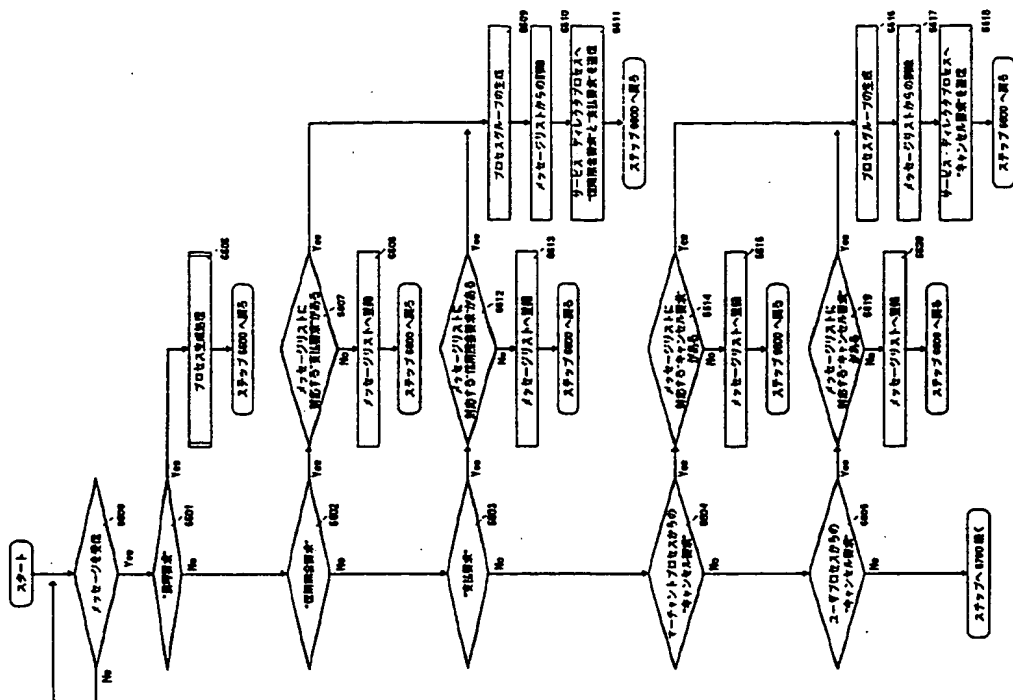


**[ 5 6 ]**

**【96圖】**

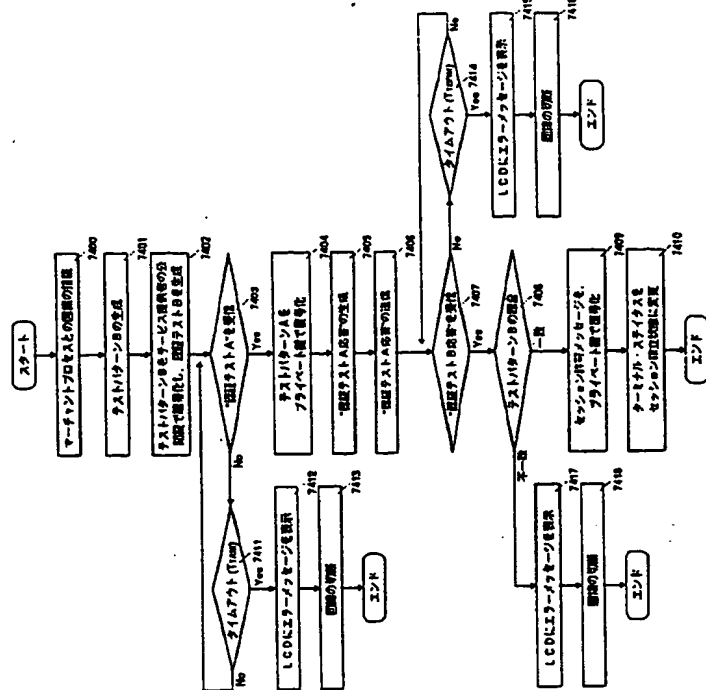


【圖97】

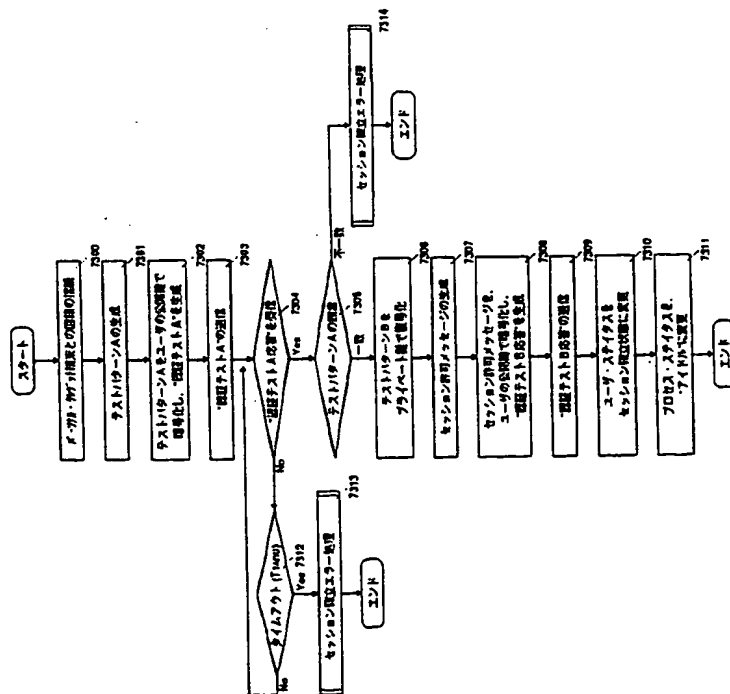




**【图105】**

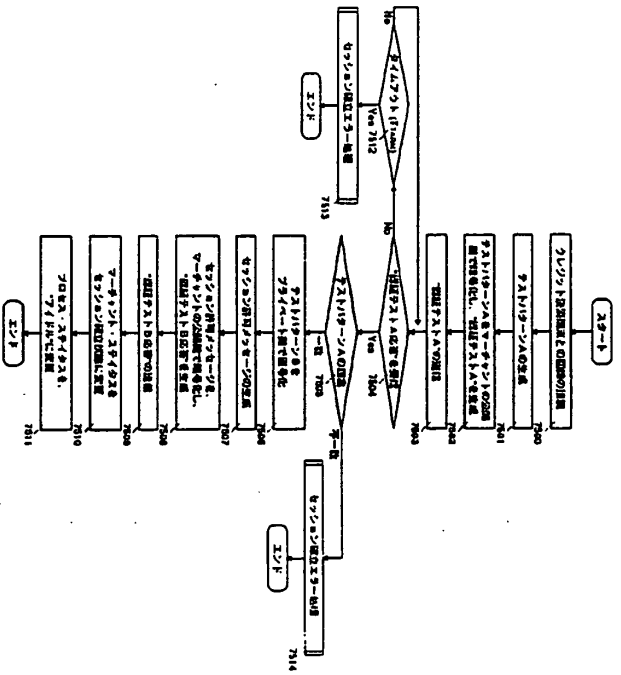


**【圖104】**



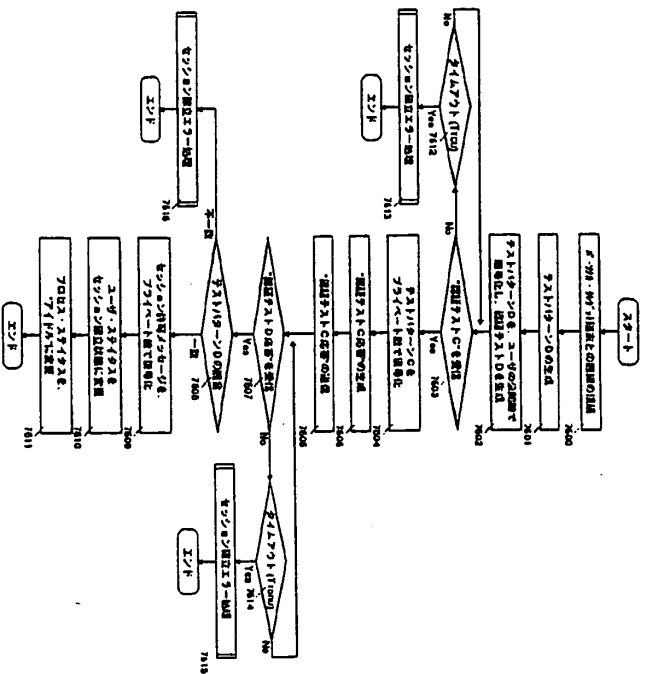
(225)

【図106】



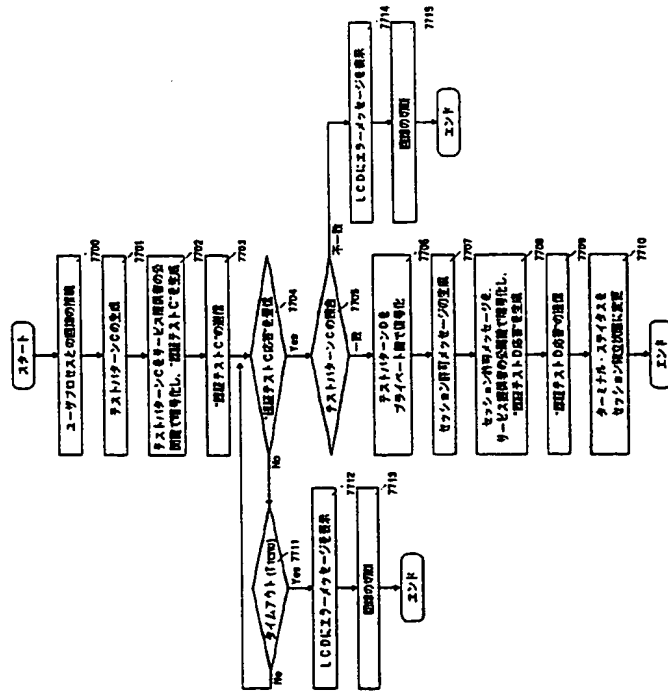
(226)

【図107】



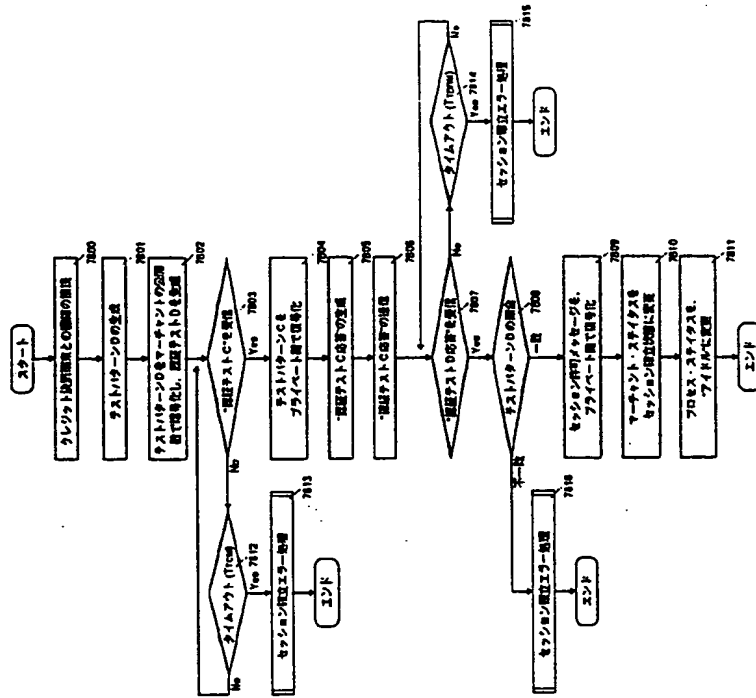
(127)

【図108】



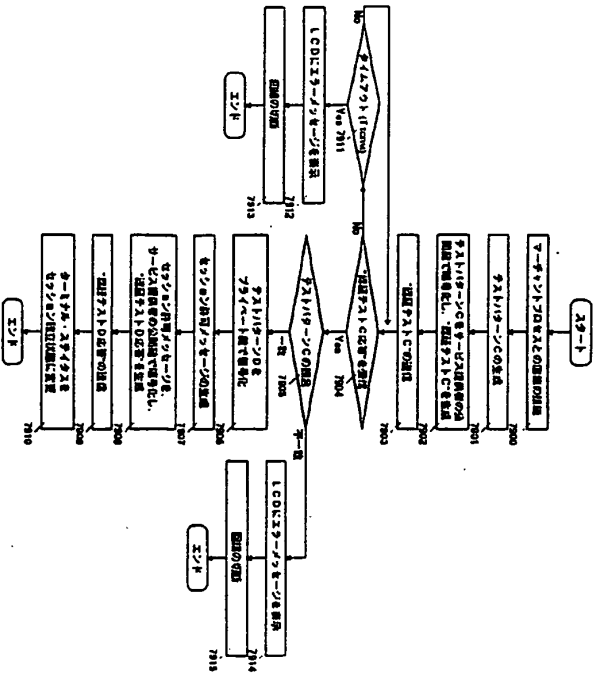
(128)

【図109】



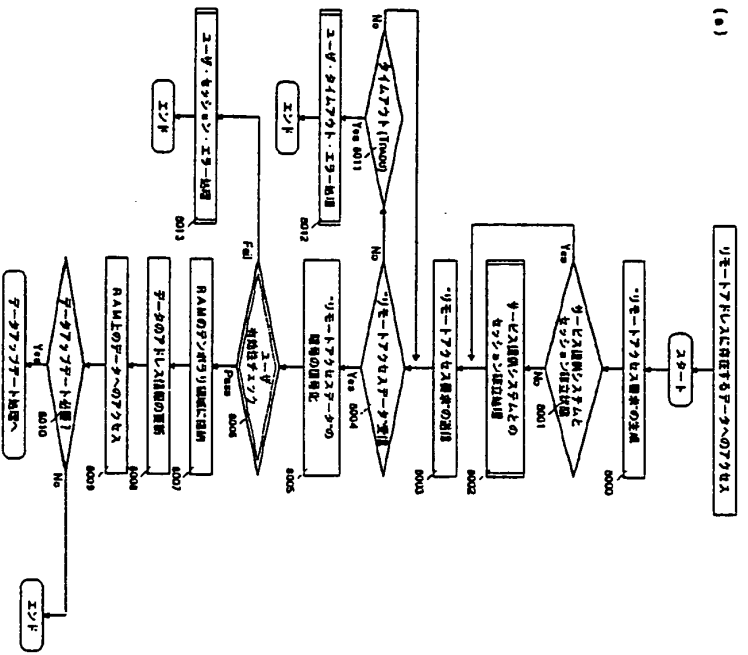
(229)

【図110】

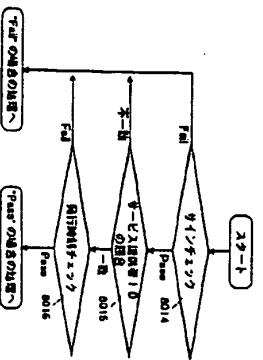


(230)

【図111】

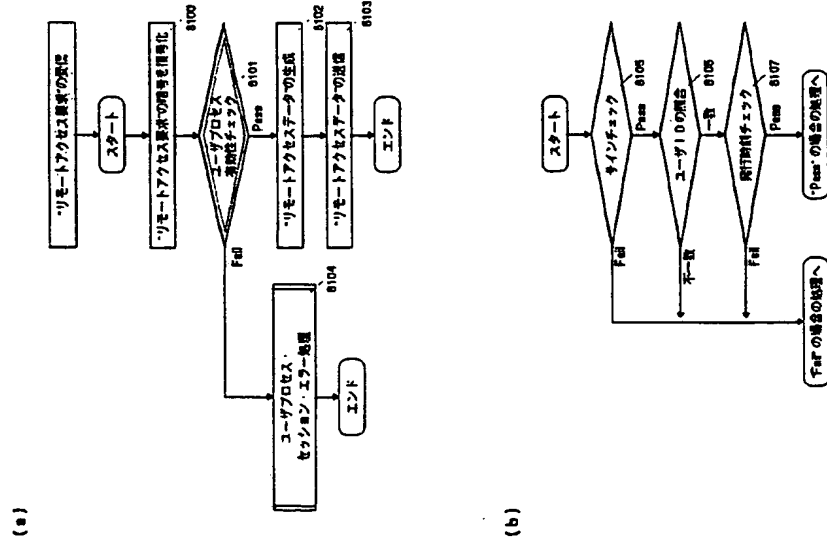


(b)



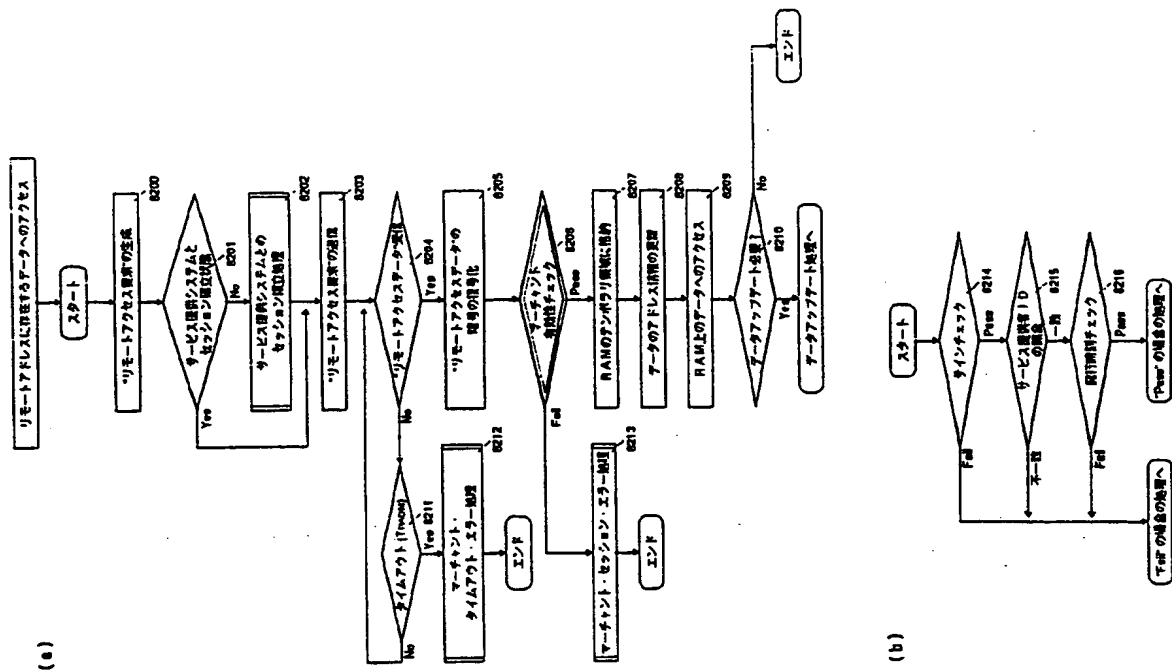
(231)

【図112】

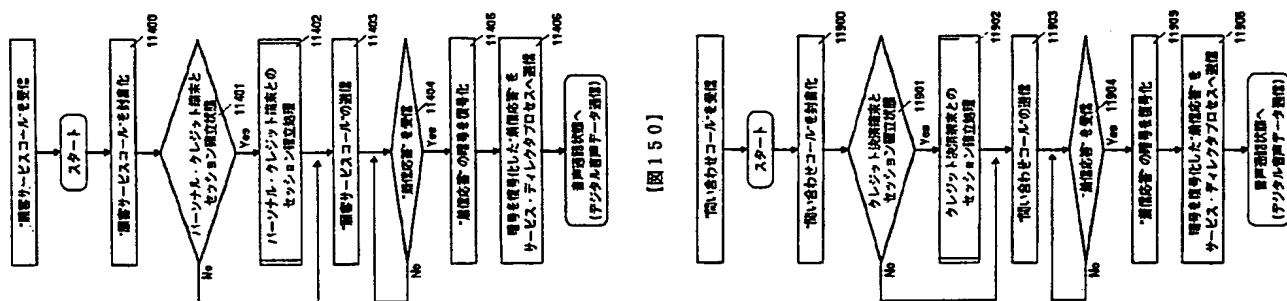


(232)

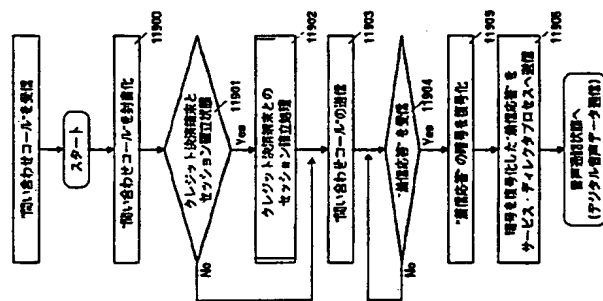
【図113】



【図145】



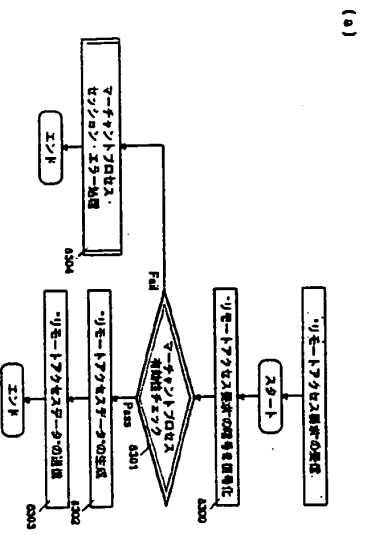
【図150】



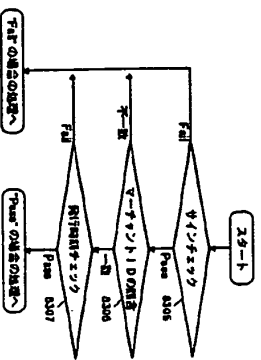


(233)

【図114】

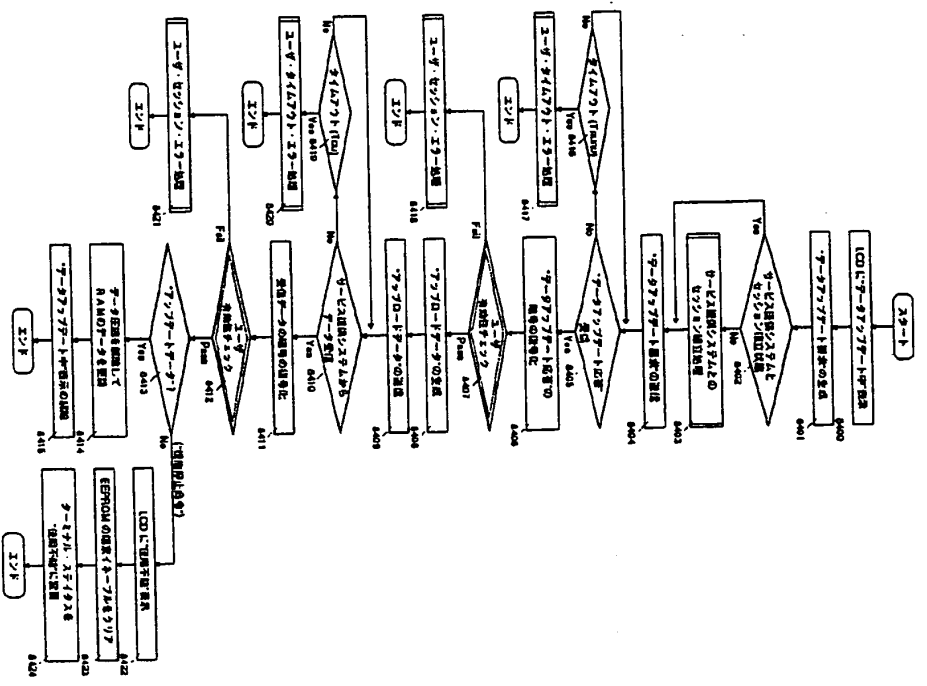


(b)



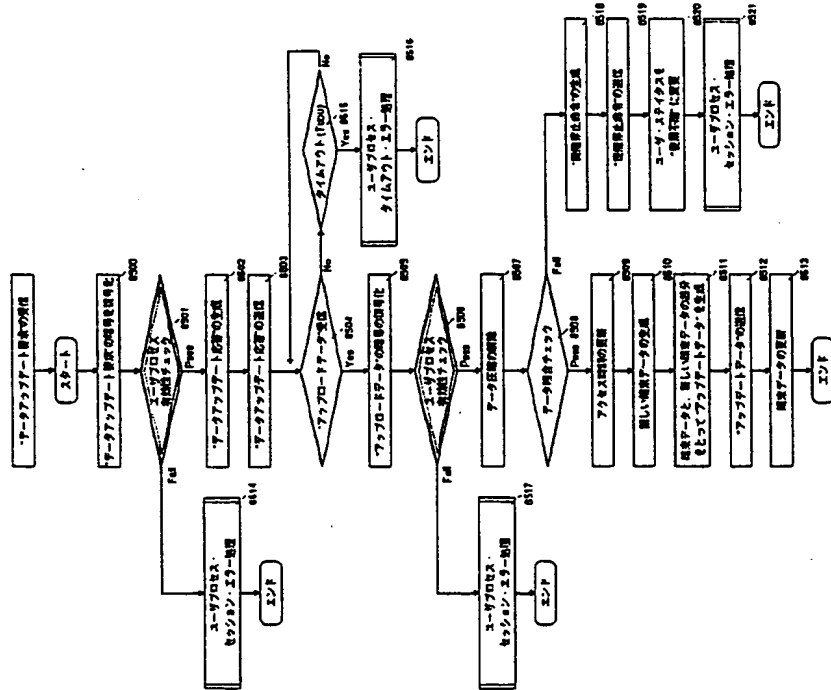
(234)

【図115】



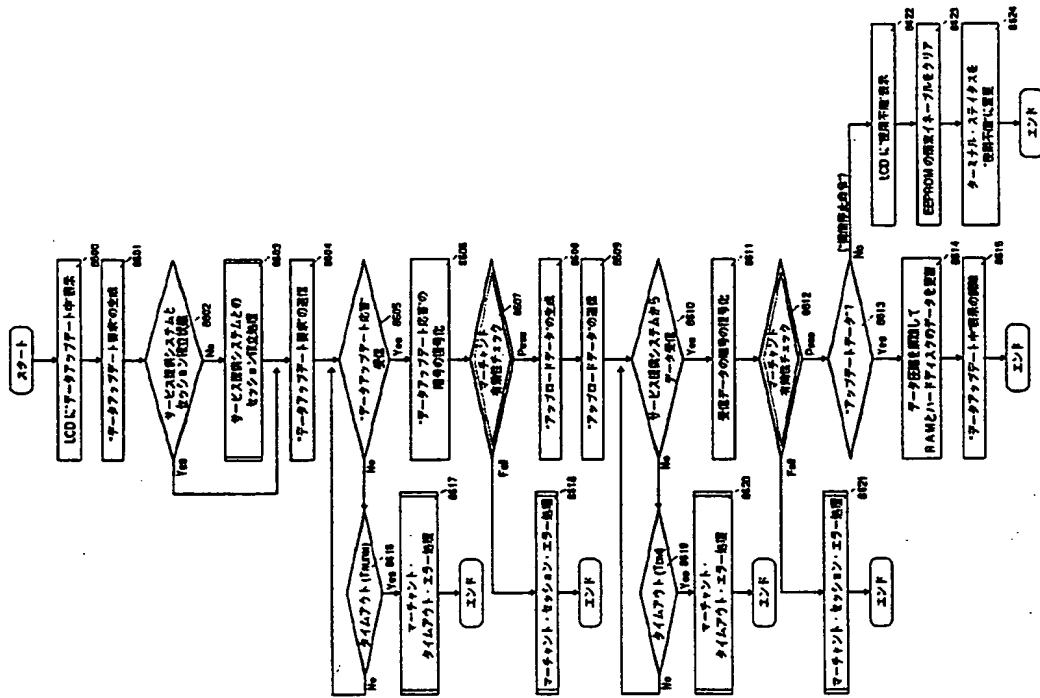
(235)

【図116】



(236)

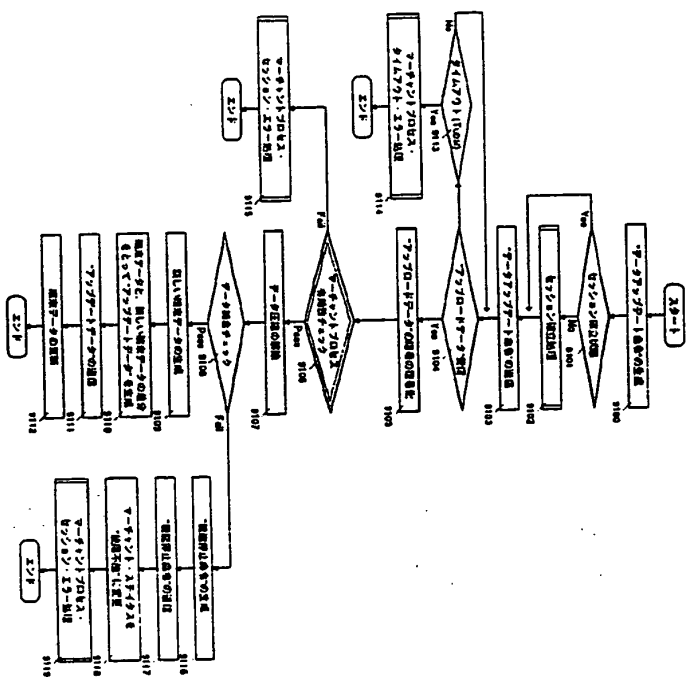
【図117】



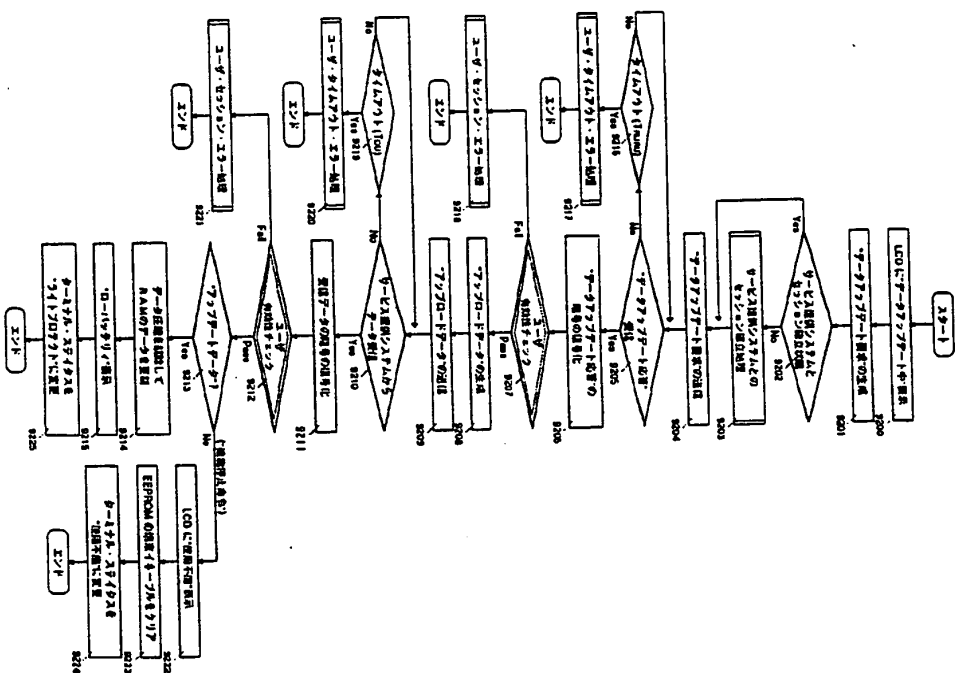




【図122】

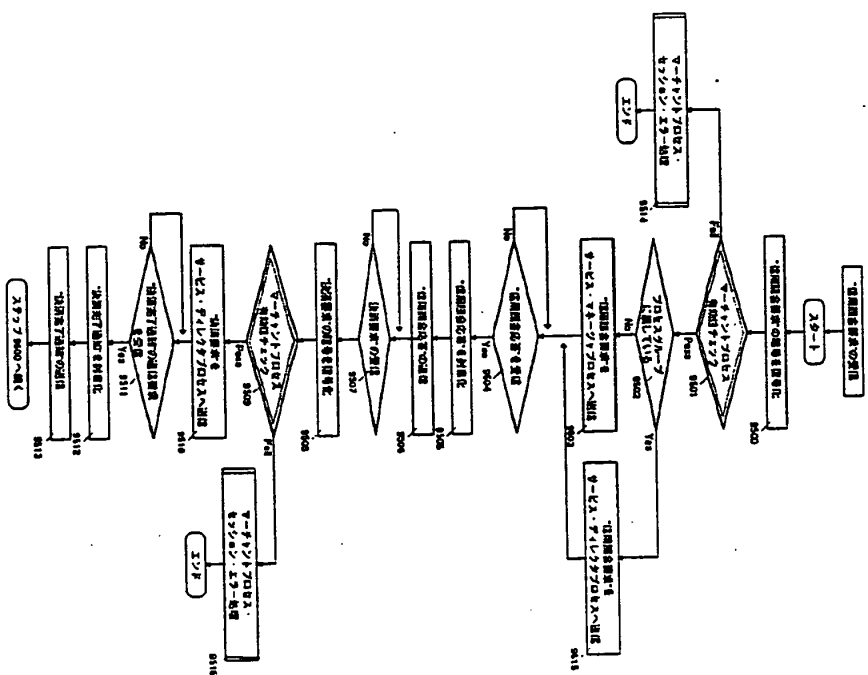


【図123】

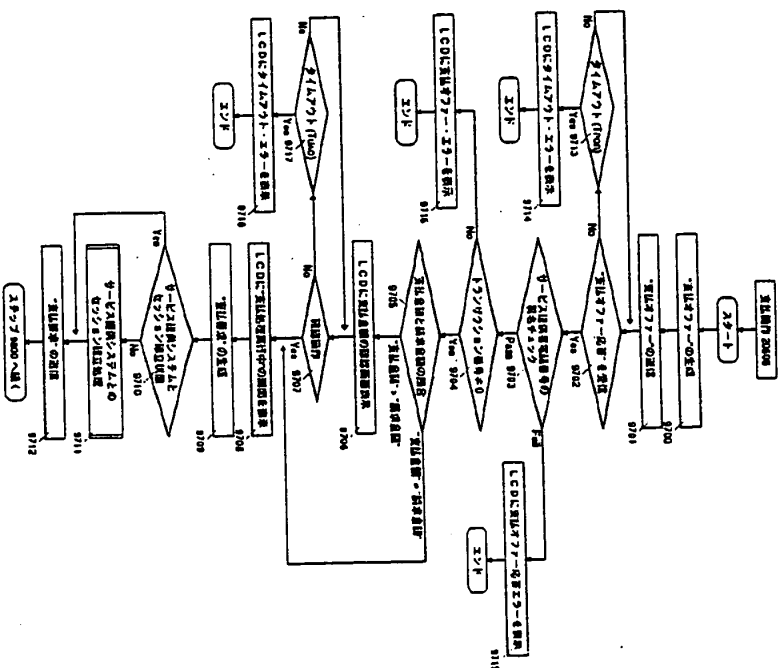




【圖 126】

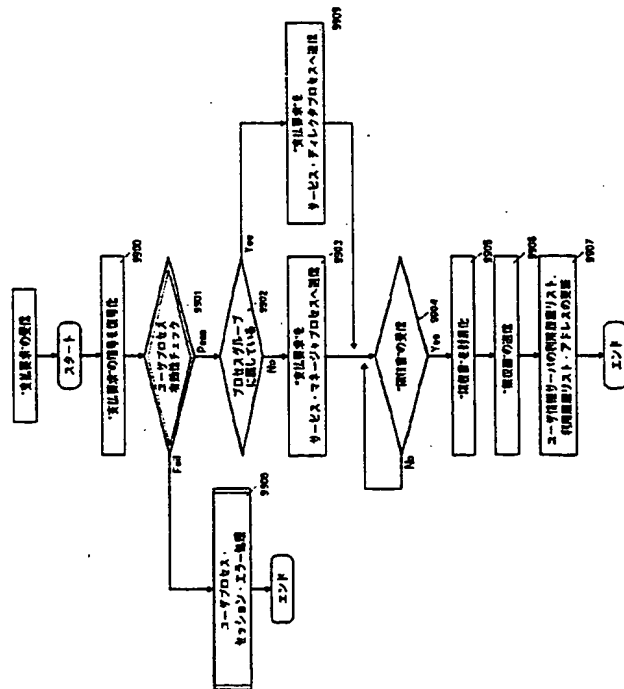


【例 128】

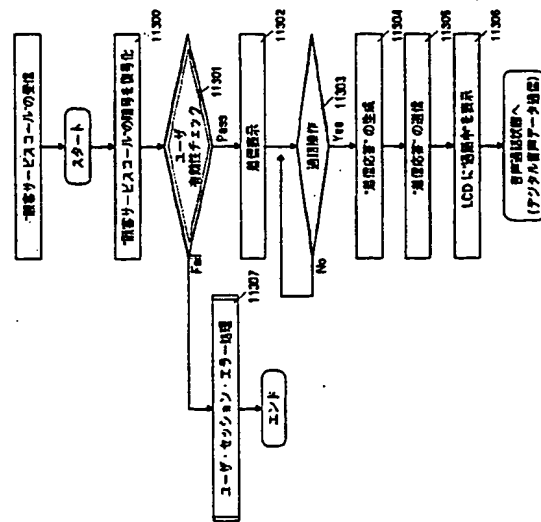


(247)

**【圖130】**

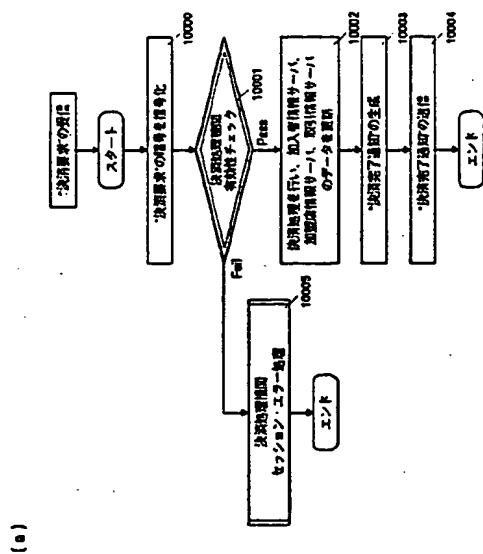


**[144]**

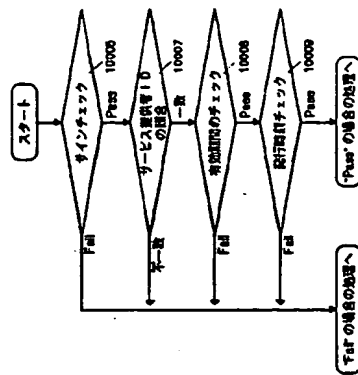


(248)

【圖131】

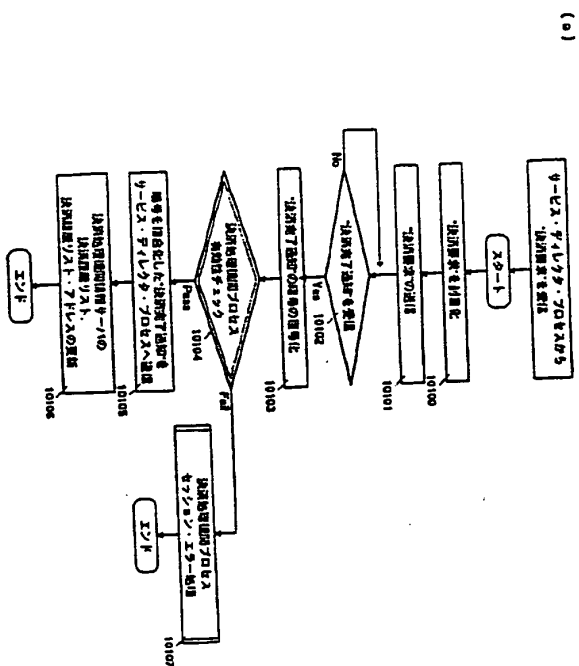


(b)



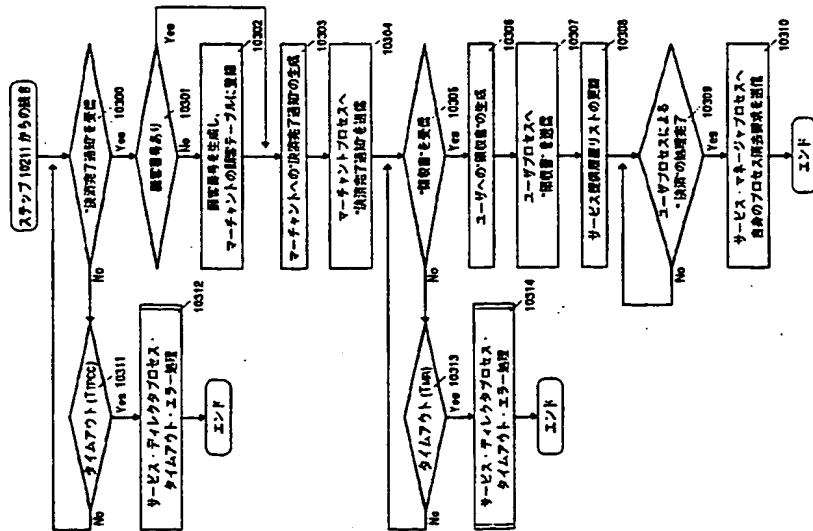


【例 132】



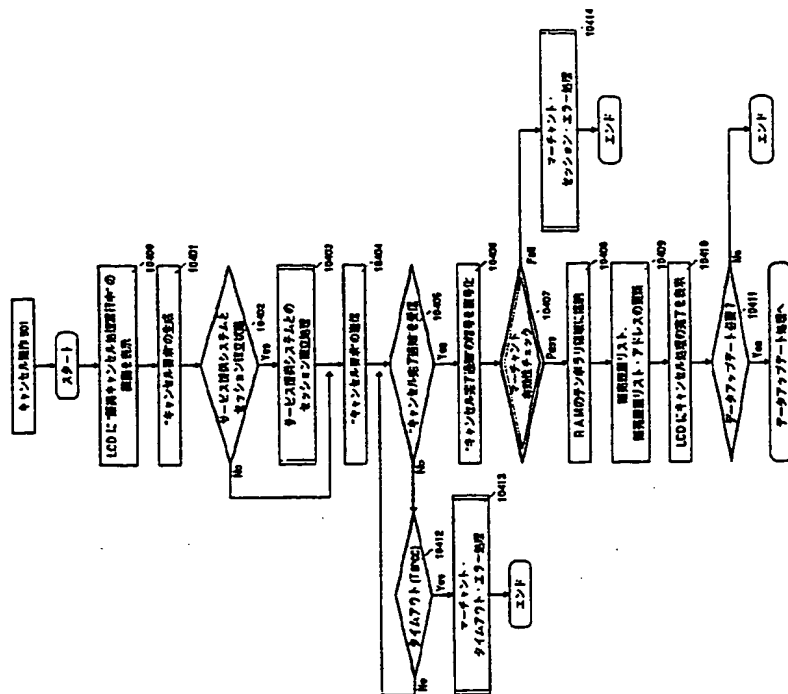
(251)

【図134】



(252)

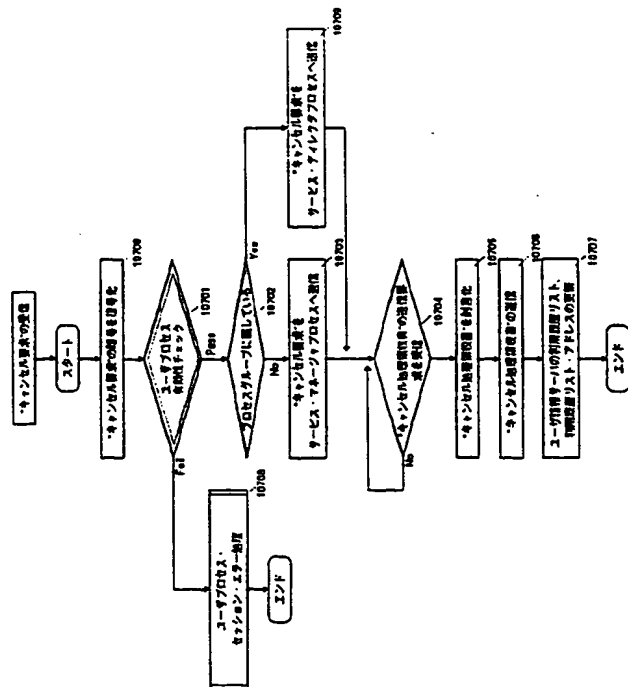
【図135】





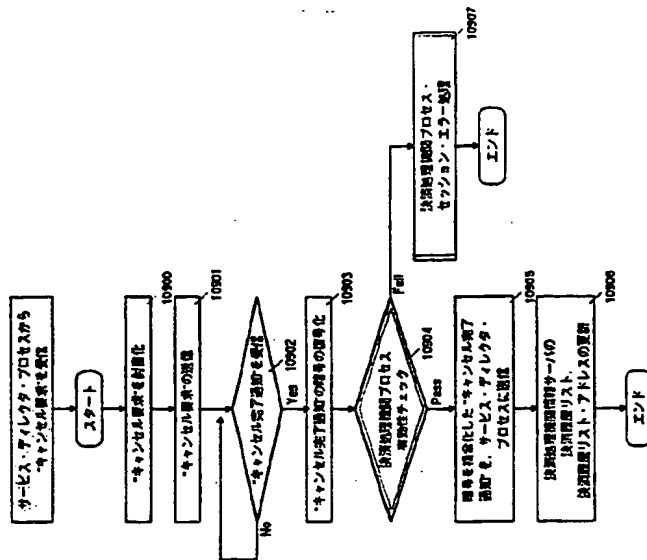
(255)

【図138】

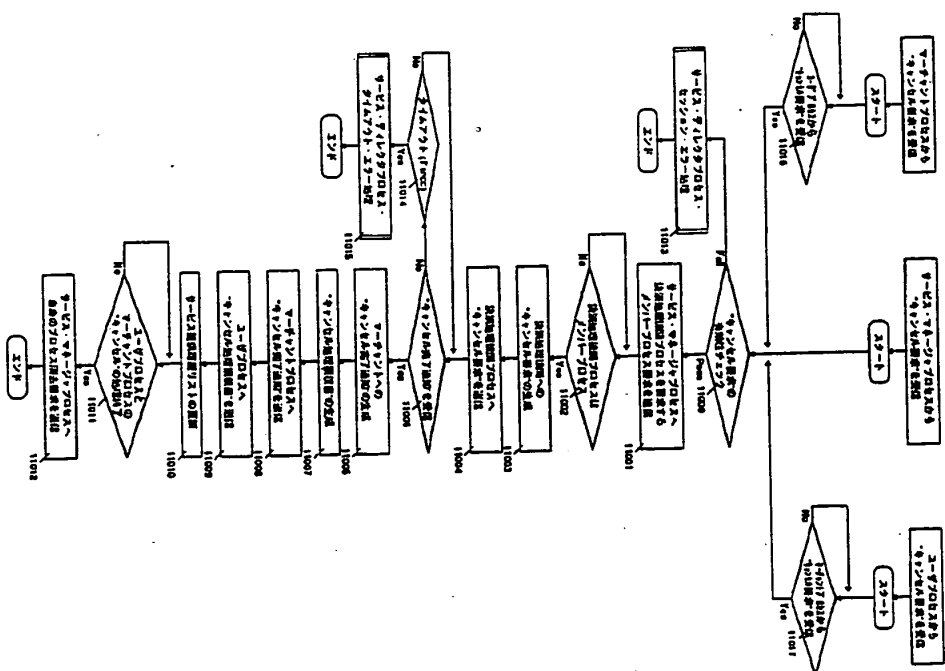


(256)

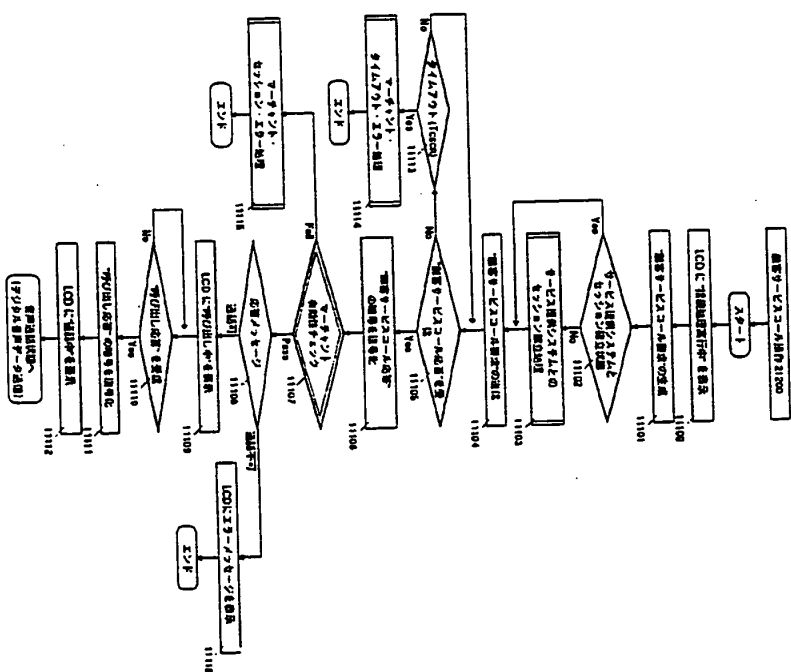
【図140】



【図141】

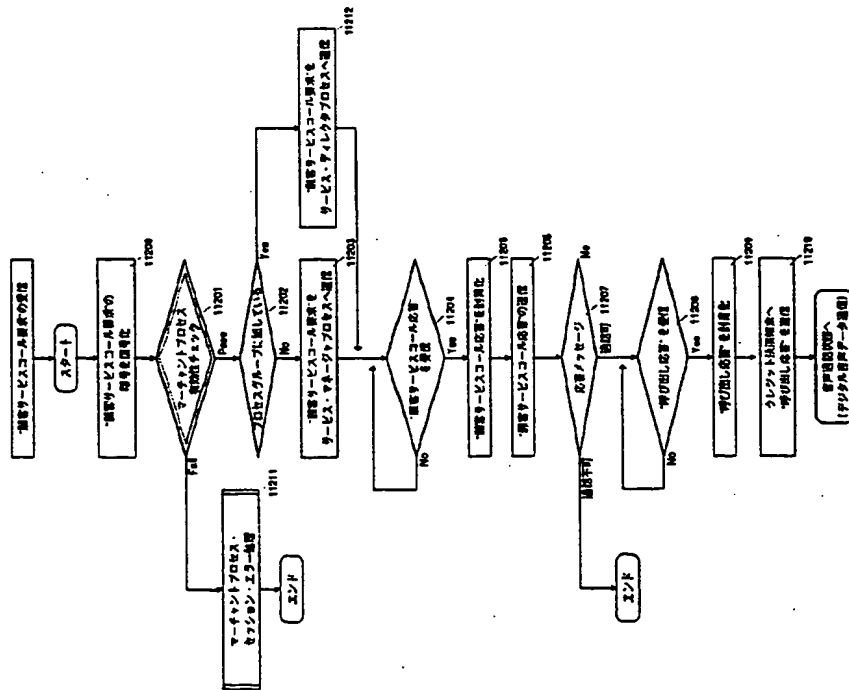


【図142】



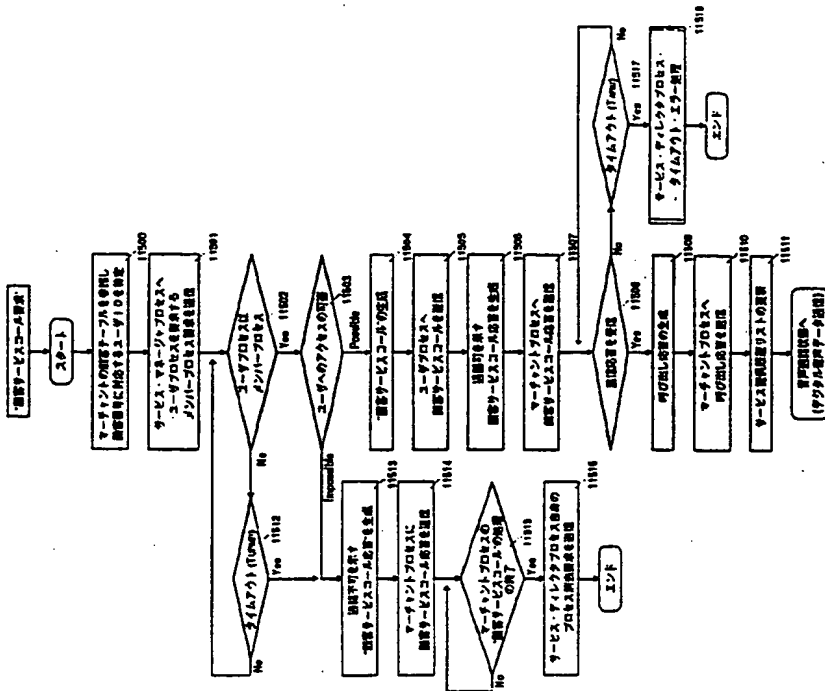
(259)

【図143】

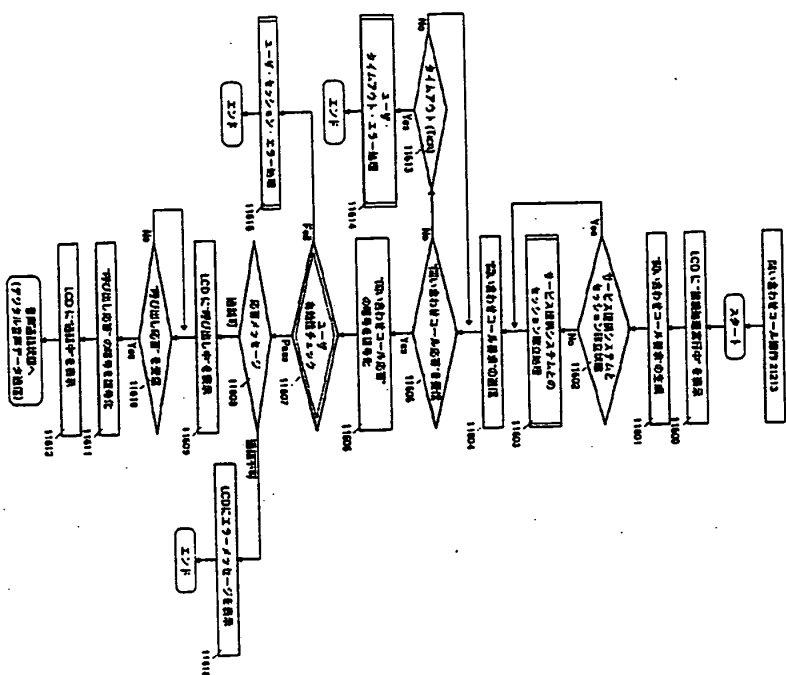


(260)

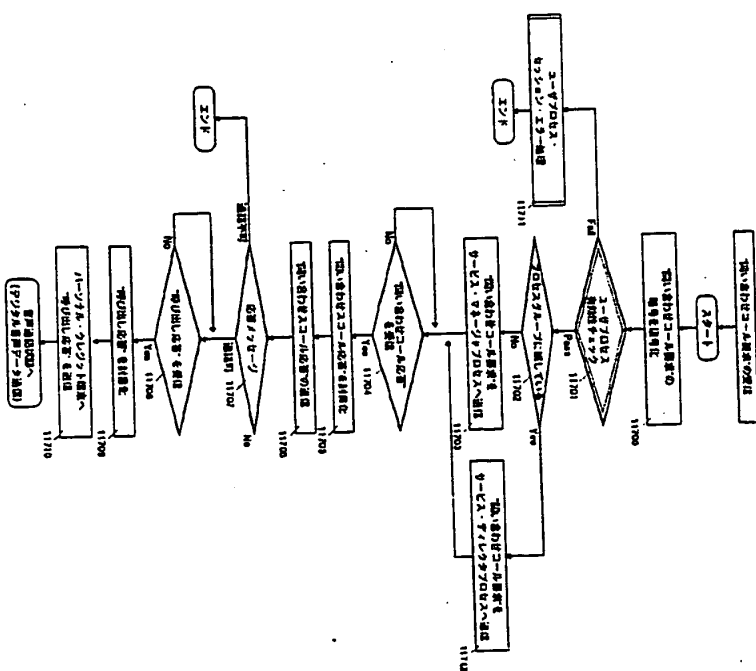
【図146】



【圖147】

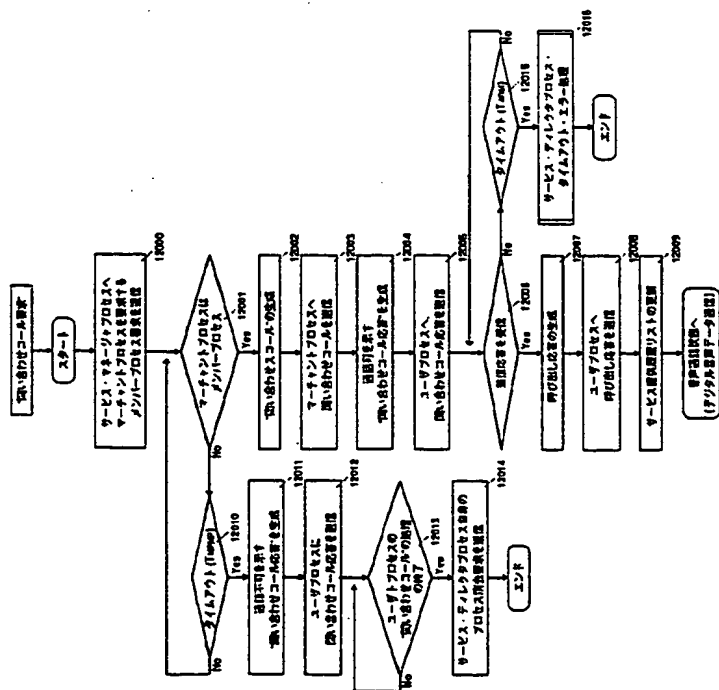


**[圖 148]**



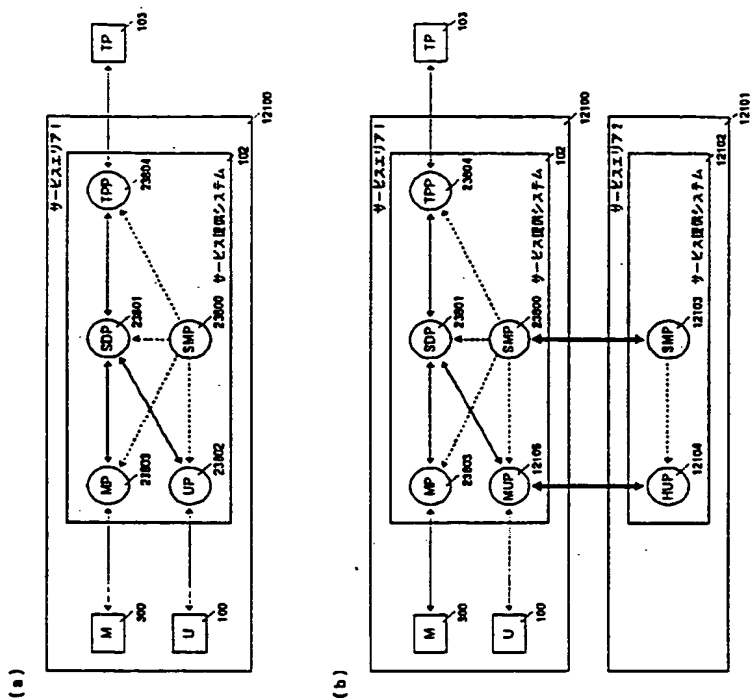
(263)

【図151】



(264)

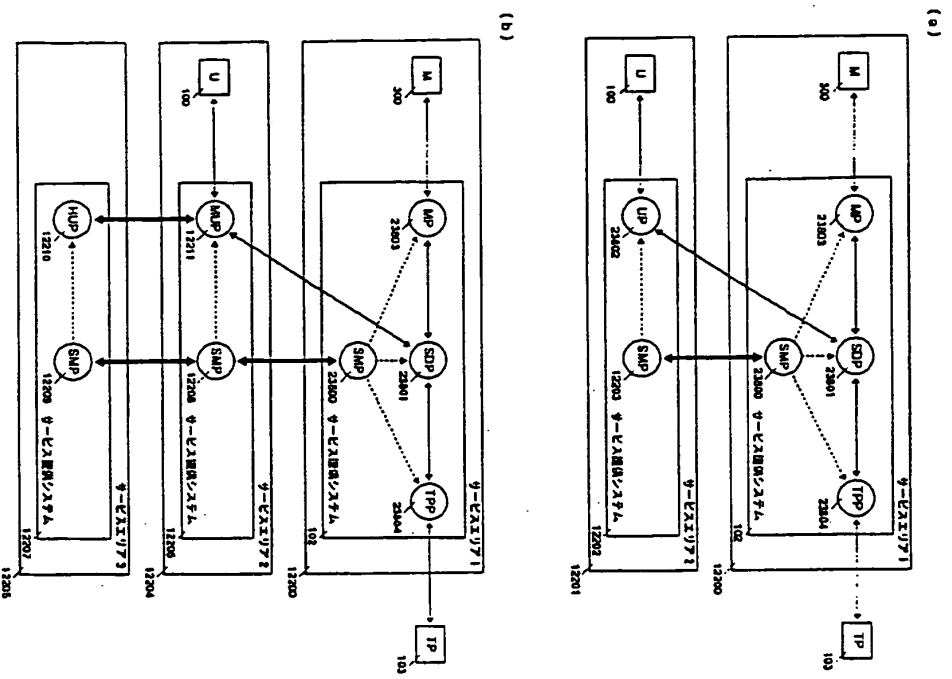
【図152】





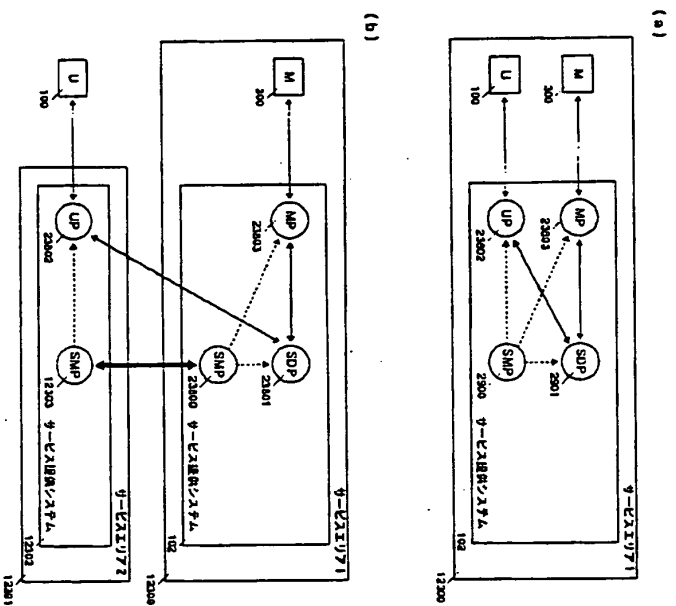
(365)

[図153]



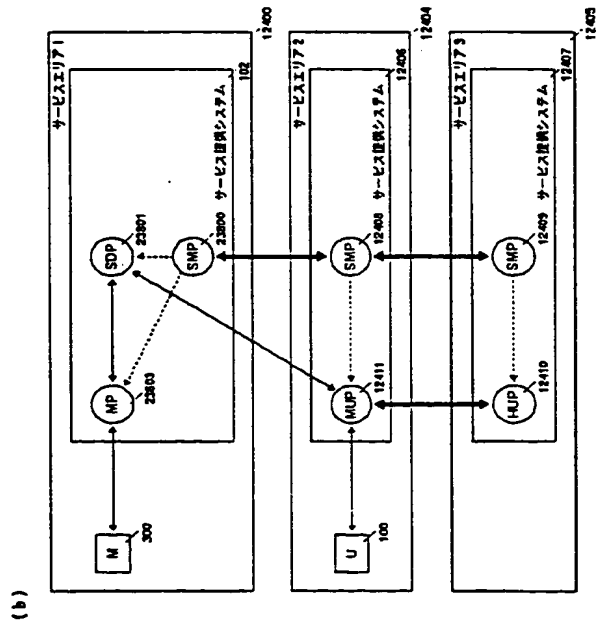
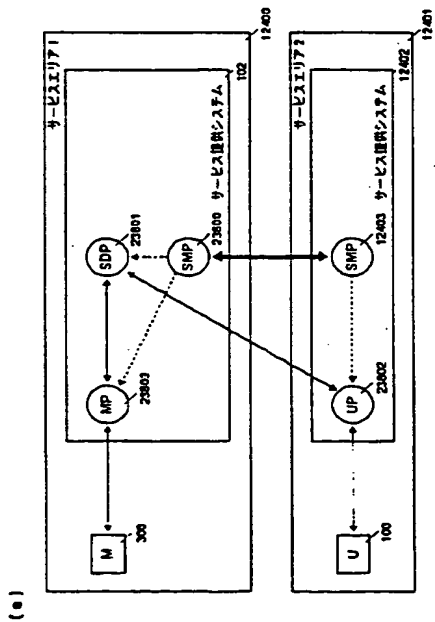
(366)

[図154]



(287)

【図155】



フロントページの続き

(S)Int.Cl. 6 F I 1104 B 1/26 109 M  
// G 0 6 F 19/00 G 0 6 F 15/30 C